取扱説明書 *Ver2.0*

Artemis
Information Security Solutions

●ご使用の際は、必ず「取扱説明書」をよくお読みの上、正しくお使いください。
●「取扱説明書」は、ご不明な点をいつでも解決できるように、すぐに取り出して見られる場所に保管してください。
●機能の向上・改良等、都合により仕様（ソフトウェア、ハードウェア、製品の外観等）は予告なく変更される可能性があります。
●最新版の「取扱説明書」は弊社Webサイトにてダウンロードいただけます。ご確認くださいますようお願い申し上げます。

安全にお使いいただくために

この取扱説明書は、製品を安全に正しくお使いいただき、お客様や他の人々への危害や財産への損害を未然に防止するための重要事項について、マーク表示が使われています。
その表示と意味は以下の通りです。内容をよく理解してから本文をお読みください。

禁止	**この表示を無視して、誤った取扱いをすると、人が死亡または重傷を負う可能性があることを示します。**
注意	**この表示を無視して、誤った取扱いをすると、人が傷害を負う可能性がある内容および物的損害のみの発生が想定される内容を示します。**

注意

正しく安全にお使いいただくために、本製品をお使いの前に必ず以下の注意事項をよくお読みください。また、ご使用の際に必ずこれらの事項をお守りください。これらの事項が守られない場合、感電、火災、故障などにより使用者の重傷または死亡につながる恐れがあります。

禁止	**異常状態のまま使用しないでください！** 煙が出たり、変な臭いや音がするなど異常状態のまま使用しないでください。 感電・火災の原因となります。 すぐに電源を切り、電源プラグをコンセントから抜いて、弊社サポート窓口にご相談ください。 お客様による修理は危険ですから絶対にしないでください。
禁止	**分解・改造・修理しないでください！** 各部のネジを外したり、カバーを開けたりしないでください。また製品内部の部品を改造・交換しないでください。異常発熱、火災、感電、事故などの原因となる恐れがあります。
禁止	**異物・液体を入れないでください！** 製品内部に異物や液体が入ると、ショートして異常発熱、誤動作、火災、感電、事故などの原因となる恐れがあります。万一異物や液体が入ってしまった場合は、電源コードをコンセントから外して弊社サポート窓口にご連絡ください。
禁止	**雷のときはさわらないでください！** 雷が発生している間は、製品各部およびケーブルにさわらないでください。感電の恐れがあります。
注意	**本製品を長時間さわらないでください！** 本製品は、機器全体が暖かくなります。通常の使用条件で問題になることはありませんが、あまり長時間さわり続けると低温やけどの恐れがあります。
注意	**接続したケーブル類を引っ張らないでください！** ケーブル類と本製品の接続部を破損する恐れがあります。また本製品を棚や机など高さのある場所に設置している場合、小型・軽量のために落下する恐れがあります。機器の破損の他、けがなどの事故の原因となります。

AC電源・電源ケーブル

禁止	**正しい電圧で使用してください！** 指定の電圧（交流100V）以外で使用すると異常発熱、火災、感電、故障などの原因となる恐れがあります。
注意	**システムを停止しないで電源を切ることは絶対にしないでください！** HDDの破損等、機器およびデータのトラブルの原因となる恐れがあります。
注意	**電源を切る際は、必ず管理画面からシステムを停止し、PWRランプの消灯を確認の上、スイッチを切ってください！** HDDの破損等、機器およびデータのトラブルの原因となる恐れがあります。
注意	**電源切断後、再投入まで5秒間以上お待ちください！** いったん電源スイッチを切ったら、すぐにスイッチを入れずに5秒間以上の間隔をあけてください。すぐに入れなおすと故障の原因となる恐れがあります。
注意	**付属のケーブル以外ご使用にならないでください！** 他の電源ケーブルを使用すると、火災や感電、故障の原因となる恐れがあります。

禁止	**電源ケーブルを傷つけないでください！** 電源ケーブルが傷んだ状態のまま使用しないでください。異常発熱、火災、感電、故障などの原因となる恐れがあります。 また以下の点を守ってケーブルを傷めないようにしてください。 ◇電源ケーブルを加工しない ◇無理に曲げたり、ねじったり、引っ張ったりしない ◇電源ケーブルの上に物を載せない ◇熱源の近くに電源ケーブルを配線しない ◇コードをかじる癖のあるペットは隔離する （かじった部分からショートし発火する危険があります） 電源ケーブルが破損したら、弊社サポート窓口にご相談ください。
禁止	**電源プラグを取り扱う際は、次の点を守ってください！** 取扱いを誤ると、火災の原因となります。 ◇電源プラグはホコリなどの異物が付着したまま差し込まない ◇電源プラグは刃の根元まで確実に差し込む
禁止	**ぬれた手で電源プラグを抜き差ししないでください！** 感電の原因となります。
禁止	**電源コンセントに電源プラグを接続したまま分解しないでください！** 感電・やけどの原因となります。
禁止	**必ずアースを接続してください！** 感電事故防止のため、必ずアース（第三種接地）を接続してください。雨や水がかかると、事故や故障の危険があります。
注意	**連休や旅行等で長期間ご使用にならないときは、安全のため必ず電源プラグをコンセントから抜いてください。**
注意	**タコ足配線や無理な配線はしないでください！** コンセントや電源タップの定格を超えて接続すると、発熱し火災につながる危険があります。

設置・移動

禁止	**屋外に設置しないでください！** 本製品は屋内専用です。屋外では絶対に使用しないでください。
禁止	**直射日光や湿度が高い場所に本製品を設置しないでください！** 異常発熱、火災、感電、故障などの原因となる恐れがあります。
禁止	**極端に低温の場所や温度差が大きい場所、結露が発生しやすい場所に本製品を設置しないでください！** 異常発熱、火災、感電、故障などの原因となる恐れがあります。

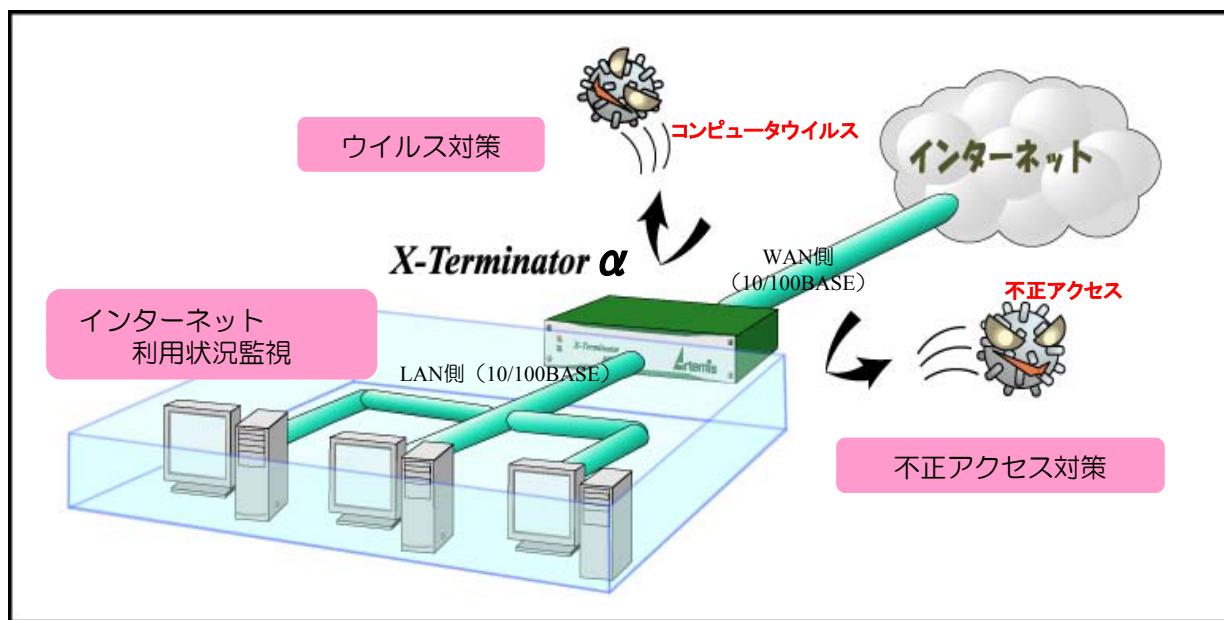
禁止	**本製品は水平に設置してください！** 不安定な場所や傾斜した場所に設置すると、転倒、落下、落下によるケガの原因となる恐れがあります。
禁止	**本製品の通風孔をふさがないでください！** 通風孔をふさぐと内部に熱がこもり、火災の危険があります。 設置する際は次の点を守ってください。 ◇押入れや本箱など風通しの悪いところには設置しない ◇じゅうたんや布団の上には設置しない ◇毛布やタオル、テーブルクロスのような布をかけない
禁止	**本製品の上に物を置かないでください！** 本体内部を圧迫する恐れがある他、内部に熱がこもり、誤動作や火災、故障の原因となる恐れがあります。
禁止	**本体の周囲20mm以上の空間を確保してください！** 隙間なく設置すると、内部に熱がこもり、誤動作や火災、故障の原因となる恐れがあります。
禁止	**ほこりや粉塵の多い場所に本製品を設置しないでください！** 異常発熱、火災、感電、故障などの原因となる恐れがあります。
禁止	**油や湯気のあたる場所に本製品を設置しないでください！** 異常発熱、火災、感電、故障などの原因となる恐れがあります。
注意	**小さなお子様の手の届く場所には、設置・保管しないでください！** 本製品の落下または転倒により、お子様がけがをする危険があります。
注意	**ペットが上に乗ったり、いたずらする恐れのある場所に設置・保管しないでください！** 毛や糞尿が製品内に入ると、故障や火災等、トラブルの原因となります。
注意	**本製品を移動する前は、電源を切り、電源プラグを抜き、すべての配線を外したことを確認してください！** 本製品を設置・移動する前に、必ず電源コードを抜いておいてください。 コードが傷つくと誤動作や火災につながる恐れがあります。
注意	**本製品の移動の際は、決して片手で持たないでください！** 落下してけがをする危険があります。必ず両手でしっかり抱え持ってください。

免責事項について

注意	**日本国以外では絶対に使用しないでください！** 本製品は日本国内での使用を前提に設計、製造しています。 国外でお使いになると電圧等の規格が異なるため、故障や火災等の事故につながる恐れがあります。絶対に日本国以外ではお使いにならないでください。
注意	**バックアップは必ず実行してください！** お使いのPCのデータは必ず定期的にバックアップを実行し、メディアは安全な場所に保管してください。 また本製品やお使いのPCの設定項目の値等、重要な情報は必ずメモをとり、安全な場所に保管してください。 かかるデータならびに情報の紛失・破損による損害について、弊社では一切の責を負いかねますので、ご了承ください。
注意	**自己責任でセキュリティ対策を行うことを強く推奨します！** サーバをインターネット上に公開する際は、その危険性を理解して、必要なセキュリティ対策を行う必要があります。 本製品はファイアウォールですが、不正アクセスの手段や抜け道（セキュリティホール）は日夜新たに発見されており、それを防ぐ完璧な手段はありません。 インターネット接続には危険がともなう事を御理解いただくとともに、常に最新の情報を入手して対処するようにしてください。
注意	**周辺機器の接続はサポート対象外となります！** プリンタポート、USBポート、RS232Cポートは、X-Terminatorで機能しない設定となっています。 これらのポートに周辺機器などを接続して本製品が故障した場合、保証対象外となる場合がございますのであらかじめご了承ください.
注意	**内部設定を変更しないでください！** 取扱説明書に記述のない手順でオペレーティングシステムやドライバ等、内部設定を変更しないでください。 不具合・故障の原因となります。また、そのような設定変更によるトラブルにつきましては、誠に申し訳ございませんがサポートの対象外とさせていただくことをご了承ください。
注意	**本製品を別の用途に転用しないでください！** 本製品はファイアウォールです。 別の用途に転用された場合は、弊社サポートの対象外となります。
注意	**ネットワーク環境によっては正しく動作しません！** 本製品はネットワーク機器として、他の機器やネットワークと接続した状態で動作しますが、他機の設定等、環境が適切でないと正しく動作しません。 例：ISP事業者のサーバ（DNS、メール）のバージョンが古い
注意	**その他の免責事項** 正しくお使いの場合でも、下記のケースは弊社サポートの対象外となります。 ◇地震、落雷、津波、洪水、台風、土砂崩れ等、天変地異による損傷、破壊、紛失 ◇戦争、革命、クーデター、各種テロ、暴動等、社会動乱による損傷、破壊、紛失 ◇火災、盗難、停電、その他事故による損傷、破壊、紛失 ◇その他、弊社の責によらない事象全般による損傷、破壊、紛失

1. 概要

本製品は、最新のセキュリティ技術を統合したセキュリティ・アプライアンスサーバです。

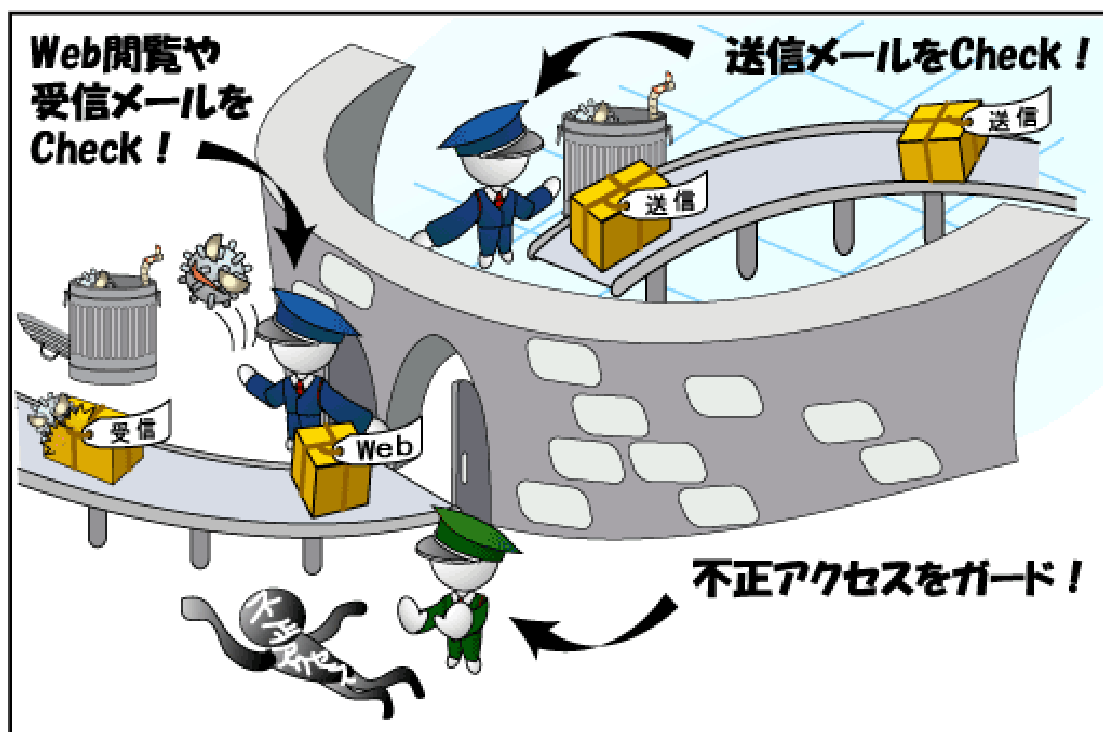
卓越したアンチウイルス機能とファイアウォール機能、インターネット利用状況の監視機能を搭載し、**HTTP・SMTP・POP3**のプロトコルでの通信をサポートしています。

注意自己責任でセキュリティ対策を行うことを強く推奨します！
サーバをインターネット上に公開する際は、その危険性を理解して、必要なセキュリティ対策を行う必要があります。
本製品はファイアウォールですが、不正アクセスの手段や抜け道（セキュリティホール）は日夜新たに発見されており、それを防ぐ完璧な手段はありません。
インターネット接続には危険がともなう事を御理解いただくとともに、常に最新の情報を入手して対処するようにしてください。

2. 特長

◆　ファイアウォール機能
お客様のネットワークに対するインターネット経由の不正アクセスをブロックします。

◆　ウイルス検知機能
ウイルスの検出・駆除をゲートウェイで実行します。ウイルスのネットワークへの侵入、また他サイトへの攻撃を阻止し、重要な情報資源やシステム資産をウイルスの脅威から守ります。

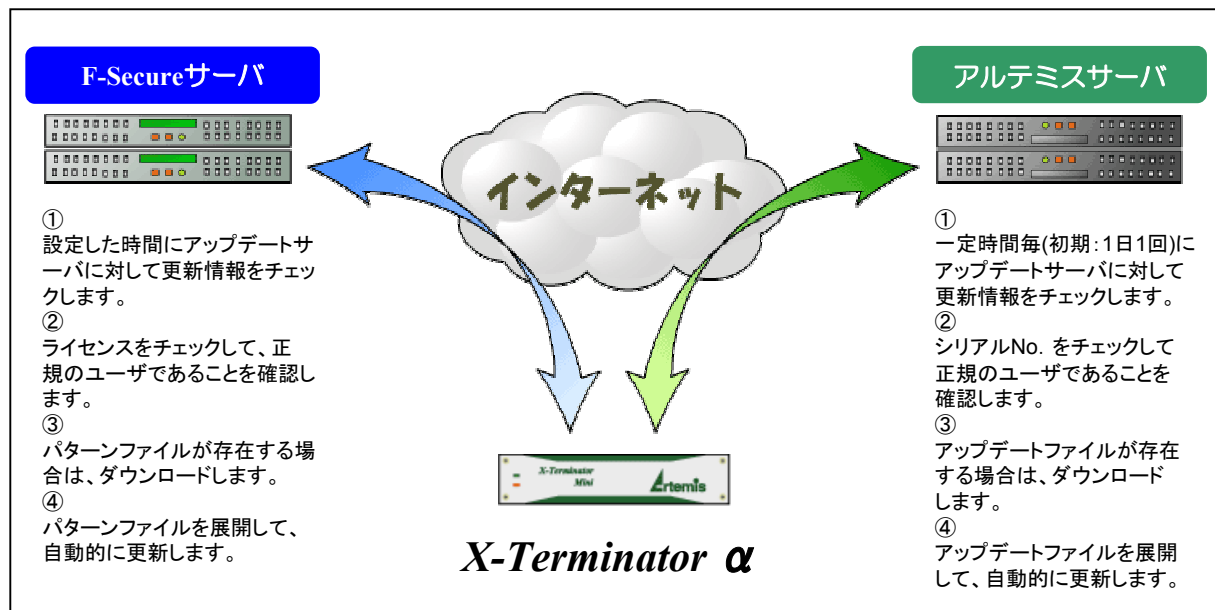
※外部からやってくるウイルスをガード Web閲覧、メールの受信時に含まれるウイルスを水際で排除することにより、クライアントの安全を確保します。
※誰かが持ち込んだウイルスをガード 万が一、ウイルスを持ち込まれた場合にも、ウイルス配信を水際で止め、あなたの信用を守ります。

対応プロトコルとしては、**HTTP、SMTP、POP3**　プロトコルに対してのウイルス検知機能をサポートします。

◆　自動アップデート機能

X-Terminator αはライセンス管理に基づき、ユーザ側に一切負担をかけない完全自動化された、２つのアップデートサービスをご提供しております。

①パターンファイルアップデート
パターンファイルのアップデートサービスは、業界にて最も更新頻度の高いフィンランドのF-Secure社を採用しています。

※F-Secure社のウイルス研究所では、新種ウイルスに対して最速の対応を行うため、毎日1、2回のパターンファイルを作成しています。***X-Terminator α***は自動的に1時間に一度確認し、差分をダウンロードすることができます。

②ファームウェアアップデート
ファームウェアのアップデートサービスは、***X-Terminator α***本体の脆弱性の修正・機能追加等を暗号化接続を利用して弊社サーバにてご提供しております。

◆　インターネット利用状況監視機能

ゲートウェイを通過するアクセスログを基に統計を出力し、インターネットの利用状況を把握することができます。

※インターネット利用状況を把握することにより、内部からの不正行為を監視し、抑止効果を発揮でき、情報漏えいリスクを軽減できます。

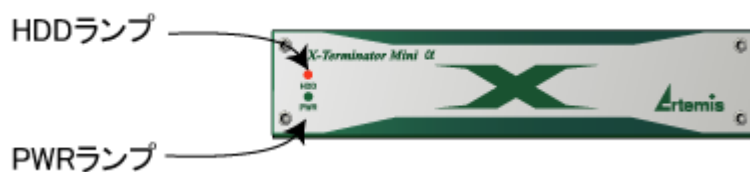
3. 梱包内容の確認

パッケージには以下の付属品が含まれていることを確認してください。

■*X-Terminator α*本体
■電源ケーブル
■取扱説明書、設置手順書（CD-ROM）
■保証書
■ゴム足
■ご使用の前に！
■簡単設定マニュアル
■ライセンス申請書№.2-2
■変更届書
■使用許諾約款

※不足品がある場合は、販売店または弊社サポート窓口にご連絡ください。

4. 各部の名称

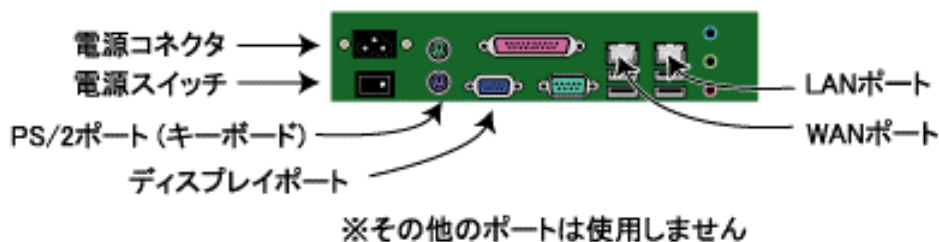
前面

■PWRランプ

本製品の動作中は緑色に点灯しています。

停止中は消灯しています。

■HDDランプ

ハードディスクにアクセス中は赤色に点滅します。

背面図

■電源コネクタ
付属の電源ケーブルを接続します。

■電源スイッチ
本製品の電源スイッチになります。

■**WAN**ポート
インターネット側のLANケーブルを接続するためのRJ-45ポートです。
10BASE-T/100BASE-TXを自動認識します。

■**LAN**ポート
社内ネットワーク側のLANケーブルを接続するためのRJ-45ポートです。
10BASE-T/100BASE-TXを自動認識します。

■ディスプレイポート
メンテナンス時、直接***X-Terminator*** αにアクセスする際、モニタを接続するために使用します。

■**PS2/**ポート（キーボード）
メンテナンス時、直接***X-Terminator*** αにアクセスする際、キーボードを接続するために使用します。

注意	**周辺機器の接続はサポート対象外となります！** プリンタポート、USBポート、RS232Cポートは、X-Terminator αで機能しない設定となっています。これらのポートに周辺機器などを接続して本製品が故障した場合、保証対象外となる場合がございますのであらかじめご了承ください。

設置前の確認事項

1. 必要環境

■コンピュータ機器

本製品は、以下のいずれかのコンピュータに対応しています。
･Windows95/98/Me/NT/2000/XPを搭載した、Ethernet（RJ45）を装備したコンピュータ。
･MacOS8.0以降を搭載し、Ethernet（RJ45）を装備したMacintosh。

■ネットワーク機器

本製品は、以下のネットワーク機器が必要となります。
・ストレートタイプのLANケーブル（UTPまたはSTP）。
・10BASE-T/100BASE-TX対応のHUBまたはスイッチングHUB。

2. ネットワーク機器の接続

■LAN側ポートの接続

ストレートタイプのLANケーブル（UTPまたはSTP）で、本製品のLAN側のポートとHUBを接続してください。

■WAN側ポートの接続

ストレートタイプのLANケーブル（UTPまたはSTP）で、本製品のWAN側のポートとADSLモデムやルータを接続してください。

※ ADSLモデムの種類によっては本製品と接続する際にストレートケーブルではなく、クロスケーブルを必要とする場合があります。
※ 10BASE-Tでの接続にはカテゴリ3以上、100BASE-TXでの接続にはカテゴリ5以上のツイストペアケーブルを使用してください。

3. 電源アダプタの接続と起動

■付属の電源ケーブルを本製品の電源コネクタに接続し、電源ケーブルのプラグをAC100Vコンセントに差し込んでください。

■本製品背面の電源スイッチを押してください。これで本製品が起動します。

禁止	**正しい電圧で使用してください！** 指定の電圧（交流100V）以外で使用すると異常発熱、火災、感電、故障などの原因となる恐れがあります。
禁止	**付属のケーブル以外ご使用にならないでください！** 他の電源ケーブルを使用すると、火災や感電、故障の原因となる恐れがあります。
禁止	**電源ケーブルを傷つけないでください！** 電源ケーブルが傷んだ状態のまま使用しないでください。 異常発熱、火災、感電、故障などの原因となる恐れがあります。 また以下の点を守ってケーブルを傷めないようにしてください。 電源ケーブルを加工しない 無理に曲げたり、ねじったり、引っ張ったりしない 電源ケーブルの上に物を載せない 熱源の近くに電源ケーブルを配線しない コードをかじる癖のあるペットは隔離する （かじった部分からショートし発火する危険があります） 電源ケーブルが破損したら、弊社サポート窓口にご相談ください。

禁止	**電源プラグを取り扱う際は、次の点を守ってください！** 取扱いを誤ると、火災の原因となります。 電源プラグはホコリなどの異物が付着したまま差し込まない 電源プラグは刃の根元まで確実に差し込む
禁止	**ぬれた手で電源プラグを抜き差ししないでください！** 感電の原因となります。
禁止	**電源コンセントに電源プラグを接続したまま分解しないでください！** 感電・やけどの原因となります。
禁止	**必ずアースを接続してください！** 感電事故防止のため、必ずアース（第三種接地）を接続してください。 雨や水がかかると、事故や故障の危険があります。
禁止	**屋外に設置しないでください！** 本製品は屋内専用です。屋外では絶対に使用しないでください。
禁止	**直射日光や湿度が高い場所に本製品を設置しないでください！** 異常発熱、火災、感電、故障などの原因となる恐れがあります。
禁止	**極端に低温の場所や温度差が大きい場所、結露が発生しやすい場所に本製品を設置しないでください！** 異常発熱、火災、感電、故障などの原因となる恐れがあります。
禁止	**本製品は水平に設置してください！** 不安定な場所や傾斜した場所に設置すると、転倒、落下、落下によるケガの原因となる恐れがあります。
禁止	**本製品の通風孔をふさがないでください。** 通風孔をふさぐと内部に熱がこもり、火災の危険があります。 設置する際は次の点を守ってください。 押入れや本箱など風通しの悪いところには設置しない じゅうたんや布団の上には設置しない 毛布やタオル、テーブルクロスのような布をかけない
禁止	**本製品の上に物を置かないでください！** 本体内部を圧迫する恐れがある他、内部に熱がこもり、誤動作や火災、故障の原因となる恐れがあります。
禁止	**本体の周囲20mm以上の空間を確保してください！** 隙間なく設置すると、内部に熱がこもり、誤動作や火災、故障の原因となる恐れがあります。

禁止	**ほこりや粉塵の多い場所に本製品を設置しないでください！** 異常発熱、火災、感電、故障などの原因となる恐れがあります
禁止	**油や湯気のあたる場所に本製品を設置しないでください！** 異常発熱、火災、感電、故障などの原因となる恐れがあります。
注意	**タコ足配線や無理な配線はしないでください！** コンセントや電源タップの定格を超えて接続すると、発熱し火災につながる危険があります。
注意	**小さなお子様の手の届く場所には、設置・保管しないでください！** 本製品の落下または転倒により、お子様がけがをする危険があります。
注意	**ペットが上に乗ったり、いたずらする恐れのある場所に設置・保管しないでください！** 毛や糞尿が製品内に入ると、故障や火災等、トラブルの原因となります。
注意	**本製品の移動の際は、決して片手で持たないでください！** 落下してけがをする危険があります。必ず両手でしっかり抱え持ってください。
注意	**本製品を移動する前は、電源を切り、電源プラグを抜き、すべての配線を外したことを確認してください！** 本製品を設置・移動する前に、必ず電源コードを抜いておいてください。 コードが傷つくと誤動作や火災につながる恐れがあります。

設定画面について

1. Rabbitwall設定メニュー

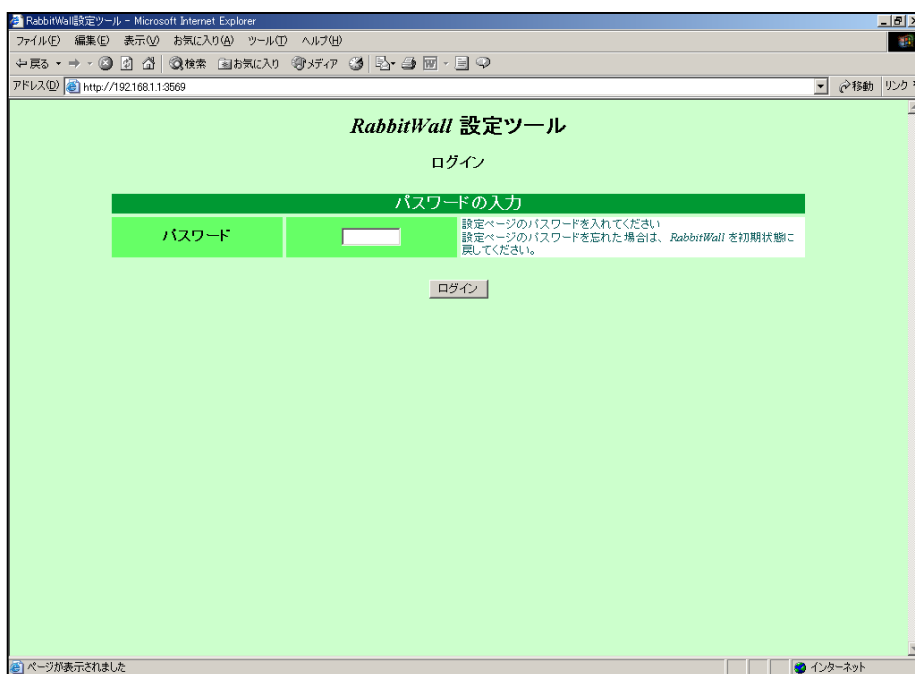
1-1. *RabbitWall* 設定ツールへのアクセス方法

本製品の設定は「Internet Explorer」や「Netscape Navigator」などのブラウザ画面から行います。
ブラウザソフトは「Internet Explorer4.0」以降、あるいは「Netscape Navigator4.0」以降をご利用下さい。
それ以前のバージョンでは、設定が正しく行われないことがあります。
ブラウザのアドレスバーに "http://192.168.1.1:3569" と入力します。

アドレス　"http://192.168.1.1:3569"

1-2. *RabbitWall*設定ツールへのログイン方法

「*RabbitWall*設定ツール」という画面が開き、「パスワード入力」と出ますので、"**rabbit**" と入力します。

パスワード　"rabbit"

メイン画面が表示されます。ここから各種設定を行います。

1-3. *RabbitWall*設定画面

メイン画面が表示されます。ここから各種設定を行います。

※インターネットへの疎通確認後、必ずこちらよりライセンス申請を行ってください。
ライセンス申請を行わないと、アップデートは出来ません。

RabbitWall設定ツール - Microsoft Internet Explorer

ファイル(F) 編集(E) 表示(V) お気に入り(A) ツール(T) ヘルプ(H)

戻る 検索 お気に入り メディア

アドレス(D) http://192.168.1.1:3569/cgi-bin/uncgi/chkPasswd.cgi 移動 Google

MENU

- ログ参照(100行)
- システム停止
- システム再起動

- フィルタ設定(WAN→LAN)
- IPポート転送(個別)設定
- IPポート転送(範囲)設定
- フィルタ設定(LAN→WAN)

- DHCP設定
- ログ設定

- ホスト設定
- グローバル設定
- ローカル設定

- パスワード設定
- 日付／時刻設定
- TOP

インターネットへの疎通確認後、必ずこちらより

ライセンス申請を行ってください。

※ライセンス申請を行わないと、アップデートは出来ません。

RabbitWall とは…

インターネット／イントラネットなどの環境において、不正アクセスなどの被害を未然に防ぎ、セキュリティシステムに関する様々な悩みをこれ1台で解決！ アルテミスが誇る高性能ファイアウォール、これが *RabbitWall* です。

<サポート>
RabbitWall 購入者の方を対象にリモートメンテナンスサポートを行っております。

・サポートセンターからのリモートメンテナンスサポート

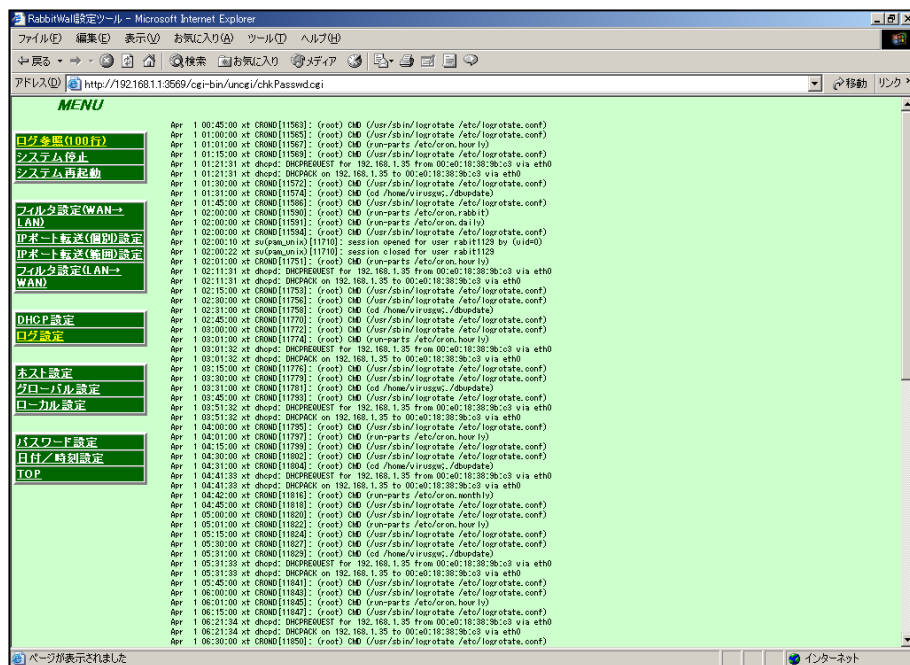
・サポートセンターでの *RabbitWall* 監視、不正アクセス時のメール送信

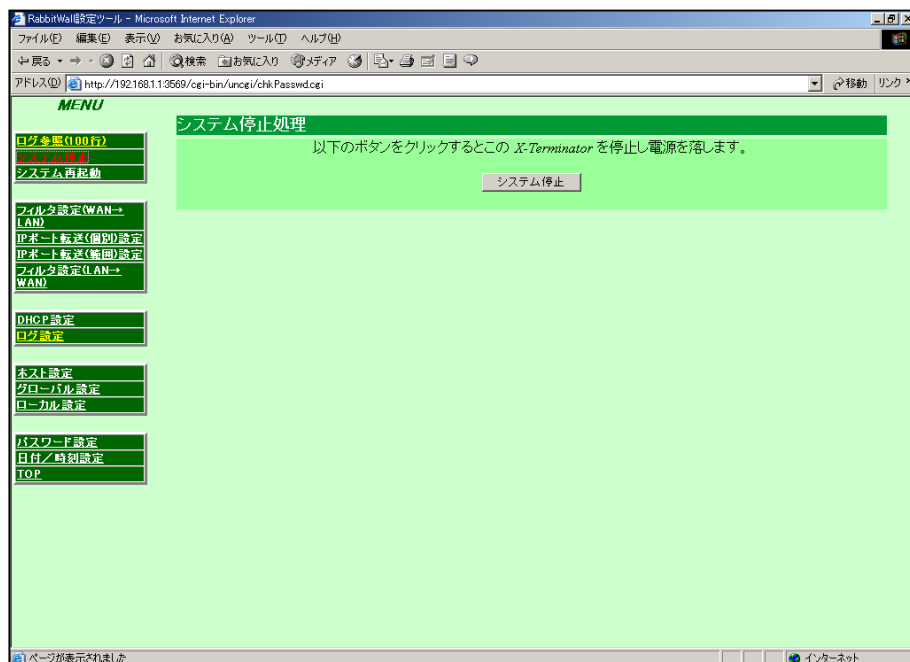
・リモートによるバージョンアップ

インターネット

内部設定を変更しないでください！
取扱説明書に記述のない手順でオペレーティングシステムやドライバ等、内部設定を変更しないでください。
不具合・故障の原因となります。また、そのような設定変更によるトラブルにつきましては、誠に申し訳ございませんがサポートの対象外とさせていただくことをご了承ください。

2. ログ参照(100行)

*X-Terminator α*に記録されている最新100行分のログが表示されます。
最新の内容に更新する場合は、最下段にある「**再読み込み**」ボタンをクリックして下さい。

3. システム停止

*X-Terminator α*のシステムを停止します。
停止までにはボタンクリック後、15秒ほどかかります。

4. システム再起動

このボタンをクリックすることで***X-Terminator α***を再起動させることができます。
停止 → 再起動までにはボタンクリック後、2分ほどかかります。

注意	**システムを停止しないで電源を切ることは絶対にしないでください！** HDDの破損等、機器およびデータのトラブルの原因となる恐れがあります。
注意	**電源を切る際は、必ず管理画面からシステムを停止し、PWRランプの消灯を確認の上、スイッチを切ってください！** HDDの破損等、機器およびデータのトラブルの原因となる恐れがあります。
注意	**電源切断後、再投入まで5秒間以上お待ちください！** いったん電源スイッチを切ったら、すぐにスイッチを入れずに5秒間以上の間隔をあけてください。 すぐに入れなおすと故障の原因となる恐れがあります。

5. フィルタ設定(WAN→LAN)

*X-Terminator α*は外部（グローバル側）からのパケットは通過できないのが基本です。
通過を許可するパケットを設定することで「ファイアウォール」に穴を開けていきます。

5-1. IPフィルタリングの設定一覧表示

現在設定されているフィルタが一覧表示されます。

ON	番号	プロトコル	ログ取得	送信元IPアドレス	送信元ポート	あて先IPアドレス	あて先ポート	適用	コメント
☐	220	udp	しない	0/0		0/0	5632		pcAnyware_8/9
☐	221	tcp	しない	0/0		0/0	5631		pcAnyware_8/9
☐	300	udp	しない	0/0		0/0	61000:65535		UDP_Stream
☐	310	tcp	しない	0/0		0/0	61000:65535		Chat (ICQ),FileTransfer (FTP,ICQ,IRC)
☐	311	udp	しない	0/0		0/0	7070:7100		RealPlayer
☐	312	tcp	しない	0/0		0/0	60200:61000		ICQ(Message)
☐	400	tcp	しない	0/0		0/0	80		fwd_www
☐	401	tcp	しない	0/0		0/0	21		fwd_ftp
☐	600	tcp	しない	0/0		0/0	113		ident
☑	610	icmp	しない	0/0	0	0/0			ping,tracert
☑	611	icmp	しない	0/0	8	0/0			ping,tracert
☐	612	udp	しない	0/0		0/0	33434:33523		tracert
☐	620	tcp	しない	0/0		0/0	1080		IRC(login)

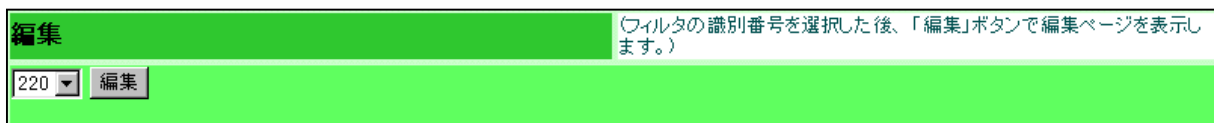
チェックの付いている項目が現在有効になっているフィルタです。
出荷時、は「icmp（ping）以外の外部からのアクセスは全て拒否する」設定になっていますので、特定のポート番号へのアクセスを「許可する」という方法で、ファイアウォール内へのアクセスが可能になります。

設定済みフィルタの有効／無効を切り替える場合、「ON」欄のチェックを必要に応じて変更し、下段にあります「適用＆保存」ボタンをクリックします。

5-2. IPフィルタリングの編集

登録済みフィルタの設定を変更できます。

変更したいフィルタ番号を選択して「編集」ボタンをクリックする事で内容が表示されます。

編集	(フィルタの識別番号を選択した後、「編集」ボタンで編集ページを表示します。)
220 ▼ 編集	

5-3. IPフィルタリングの追加

新規にフィルタの設定を追加できます。

追加	（各フィルタ項目を設定した後、「追加」ボタンで設定内容を追加してください。）		
番号	プロトコル TCP	ログ取得 しない	コメント
	送信元IPアドレス		送信元ポート
	あて先IPアドレス		あて先ポート 1024:65535
追加			

追加したフィルタはそのまま有効になりますので、フィルタを一時的に無効にする場合は「IPフィルタリングの設定一覧表示」にてフィルタのチェックを外して無効に設定して下さい。

■番号

1～999までの番号を任意で設定します。

■プロトコル

TCP、UDP、ICMP、GREから選択します。

■ログ参照

ログを記録するかどうかを設定します。
（ログがあふれますので、UDPのログはONにしないでください）

■コメント

設定するフィルタのコメントを半角文字で入力できます。
半角英数字および - . , _ / ( ) @ が使用可能です。

■送信元IPアドレス

パケットの送信元IPアドレス、またはホスト名を入力します。
“0/0”または空欄にすると、すべてのアドレスを指定したことになります。

■送信元ポート

パケットの送信元ポート番号を入力します。
プロトコルがICMPの場合、ICMPタイプを指定できます。
「開始ポート:終了ポート」のように範囲を指定でき、 空欄にするとすべてのポート、またはICMPタイプを指定したことになります。
プロトコルがGREの場合、送信元ポート指定はありませんので空欄にしてください。

■あて先IPアドレス

パケットのIPアドレスまたはホスト名を入力します。
ネットワークアドレスを入力することも可能です。
「0/0」または空欄にするとすべてのアドレスを指定したことになります。

■あて先ポート

パケットのあて先ポート番号を入力します。
プロトコルがICMPの場合、ICMPコードを指定できます。
「開始ポート:終了ポート」のように範囲を指定でき、 空欄にするとすべてのポート、またはICMPタイプを指定したことになります。
プロトコルがGREの場合、あて先ポート指定はありませんので空欄にしてください。

5-4. IPフィルタリングの削除
設定されているフィルタを削除します。
削除したフィルタの設定を再度利用する場合は、「追加」から再度設定して下さい。

削除 (フィルタの識別番号を選択した後、「削除」ボタンで削除します。)
220 削除

5-5. IPフィルタリングの初期化
フィルタリングの設定を初期状態に戻します。

「デフォルトに戻す」をクリックすると確認画面が表示されますので、初期状態に戻したい場合は「はい」をクリッして下さい。

6. IPポート転送(個別)設定

外部（グローバル側）から特定のポートに対して届いたパケットを、内部（ローカル側）の指定したホストのポートに転送する設定を行います
※IPポート転送の設定を有効にする場合は、「IPフィルタリングの設定」画面で、対応するパケットの通過を許可して下さい。

6-1. IPポート転送の設定一覧表示

現在設定されているIPポート転送の設定が一覧表示されます。

「ON」欄にチェックの付いている項目が現在有効になっている設定です。
設定されているIPポート転送の有効／無効を切り替える場合には、「ON」欄のチェックを必要に応じて変更し、下段にある「適用＆保存」ボタンをクリックする事で有効になるIPポート転送の設定が変更されます。

6-2. IPポート転送の編集

登録済みのポート転送の設定を変更できます。

変更したいフィルタ番号を選択して「編集」ボタンをクリックする事で内容が表示されます。

6-3. IPポート転送の追加

新規にポート転送の設定を追加できます。

追加 (各項目を設定した後、「追加」ボタンで設定内容を追加してください。)

番号	プロトコル TCP	コメント
	受信IPアドレス me	受信ポート
	転送先IPアドレス	転送先ポート

追加

追加した設定はそのまま有効になりますので、設定を一時的に無効にする場合は、「IPフィルタリングの設定一覧表示」からフィルタを無効に設定して下さい。

■番号

1～999までの番号を任意で設定します。

■プロトコル

TCP、UDP、ICMP、GREから選択します。

■コメント

設定するフィルタのコメントを半角文字で入力できます。
英数字および - . , _ / ( ) @ が使用可能です。

■受信IPアドレス

パケットの受信IPアドレスを入力します。
自局アドレス（グローバル側のアドレス）を指すキーワードとして「me」が使えます。

■受信ポート

パケットの受信ポート番号を入力します。
プロトコルがGREの場合、受信ポート指定はありませんので空欄にしてください。
入力しても無効になります。

■転送先IPアドレス

パケットの転送先IPアドレスを入力します。

■転送先ポート

パケットの転送先ポート番号を入力します。
プロトコルがGREの場合、転送先ポート指定はありませんので空欄にしてください。

6-4. IPポート転送の削除
設定されているポート転送の設定を削除します。

削除したフィルタの設定を再度利用する場合は、「追加」から再度設定して下さい。

6-5. IPポート転送の初期化
IPポート転送の設定を初期状態に戻します。

「デフォルトに戻す」をクリックすると確認画面が表示されますので、初期状態に戻したい場合は
「はい」をクリッして下さい。

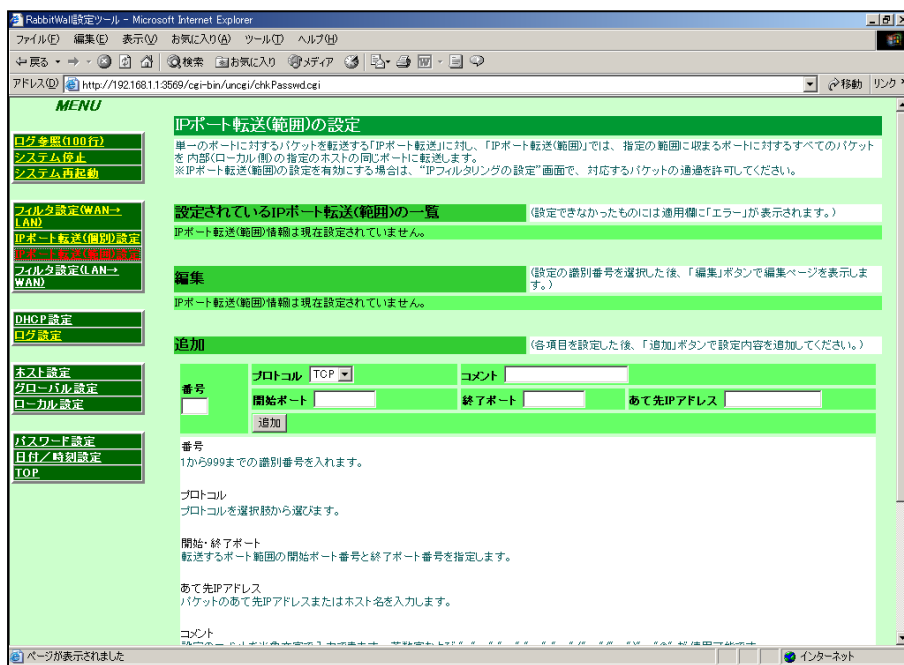
7. IPポート転送(範囲)設定

指定した範囲に収まるすべてのパケットを、内部（ローカル側）の指定したホストへ転送します。
（ポート番号はそのまま転送されます）。

※IPポート転送（範囲）の設定を有効にする場合は、「IPフィルタリングの設定」画面で、対応するパケットの通過を許可して下さい。

初期出荷状態では、「ポート転送設定(範囲)」は一つも設定されていないため、「IPポート転送(一覧)」、「IPポート転送(編集)」、「IPポート転送(削除)」は「IPポート転送（範囲）」情報は現在設定されていません。」という表示になります。

7-1. IPポート転送（範囲）の設定一覧表示

現在設定されているIPポート転送（範囲）の設定が一覧表示されます。

「ON」欄にチェックの付いている項目が現在有効になっている設定です。
チェックの入っていない項目は、設定はされているものの有効にはなっていない設定です。
初期設定の段階では、設定が入っていない状態のため、「IPポート転送（範囲）情報は現在設定されておりません。」という表示となります。

7-2. IPポート転送（範囲）の編集
現在登録されているIPポート転送（範囲）の設定を変更できます。

編集	(設定の識別番号を選択した後、「編集」ボタンで編集ページを表示します。)
IPポート転送(範囲)情報は現在設定されていません。	

変更したいIPポート転送（範囲）の番号を選択して「編集」ボタンをクリックします。
選択したIPポート転送（範囲）の設定が表示されるので、変更したい箇所を変更して「保存」ボタンをクリックすると、内容を変更できます。

7-3. IPポート転送（範囲）の追加
新規にIPポート転送（範囲）の設定を追加できます。

追加		(各項目を設定した後、「追加」ボタンで設定内容を追加してください。)	
番号	プロトコル TCP	コメント	
	開始ポート	終了ポート	あて先IPアドレス
	追加		

追加する内容を記入して「追加」ボタンをクリックすると、フィルタが追加されます。
追加した設定はそのまま有効になりますので、IPポート転送（範囲）を一時的に無効にする場合は、「IPポート転送（範囲）の設定一覧表示」から設定を無効にして下さい。

■番号
1～999までの番号を任意で設定します。

■プロトコル
TCP、UDP、ICMP、GREから選択します。

■コメント
設定するフィルタのコメントを半角文字で入力できます。
半角英数字および - . , _ / ( ) @ が使用可能です。

■開始・終了ポート
転送するポート範囲の開始ポート番号と終了ポート番号を指定します。

■あて先IPアドレス
パケットのあて先IPアドレスまたはホスト名を入力します。

7-4. IPポート転送（範囲）の削除

設定されているポート転送の設定を削除します。

削除	(設定の識別番号を選択した後、「削除」ボタンで削除します。)
IPポート転送(範囲)情報は現在設定されていません。	

削除したフィルタの設定を再度利用する場合は、「追加」から再度設定して下さい。

7-5. IPポート転送（範囲）の初期化

IPポート転送（範囲）の設定を初期状態に戻します。

設定をクリアする	(IPポート転送(範囲)の設定をクリアします。)
設定をクリアする	

「デフォルトに戻す」をクリックすると、本当にデフォルトの状態に戻していいかどうか確認表示があります。

「はい」ボタンをクリックすると、IPポート転送（範囲）の設定は初期状態にセットされます。

8. フィルタ設定(LAN→WAN)設定

内部（ローカル側）から外部（グローバル側）への接続を禁止させる パケットフィルタリングルール
の設定を行います 。

8-1. IPフィルタリングの設定一覧表示

現在設定されているフィルタが一覧表示されます。
「ON」欄にチェックの付いている項目が現在有効になっているフィルタです。
設定済みフィルタの有効／無効を切り替える場合、「ON」欄のチェックを必要に応じて変更し、
下段にあります「適用＆保存」ボタンをクリックします。

8-2. IPフィルタリングの編集

登録済みフィルタの設定を変更できます。
変更したいフィルタ番号を選択して「編集」ボタンをクリックする事で内容が表示されます。

編集	(フィルタの識別番号を選択した後、「編集」ボタンで編集ページを表示します。)
220 編集	

8-3. IPフィルタリングの追加

新規にフィルタの設定を追加できます。

追加	（各フィルタ項目を設定した後、「追加」ボタンで設定内容を追加してください。）	
番号	プロトコル TCP	ログ取得 しない	コメント
	送信元IPアドレス	送信元ポート
	あて先IPアドレス	あて先ポート 1024:65535
追加		

追加したフィルタはそのまま有効になりますので、フィルタを一時的に無効にする場合は、「IPフィルタリングの設定一覧表示」からフィルタのチェックを外して無効に設定して下さい。

■番号

1～999までの番号を任意で設定します。

■プロトコル

TCP、UDP、ICMP、GREから選択します。

■ログ参照

ログを記録するかどうかを設定します。
（ログがあふれますので、UDPのログはONにしないでください）

■コメント

設定するフィルタのコメントを半角文字で入力できます。
英数字および - . , _ / ( ) @ が使用可能です。

■送信元IPアドレス

パケットの送信元IPアドレス、またはホスト名を入力します。
“0/0”または空欄にすると、すべてのアドレスを指定したことになります。

■送信元ポート

パケットの送信元ポートまたはサービス名を入力します。
プロトコルがICMPの場合、ICMPタイプを指定できます。
「開始ポート:終了ポート」のように範囲を指定でき、空欄にするとすべてのポートまたはICMPタイプを指定したことになります。
プロトコルがGREの場合、送信元ポート指定はありませんので空欄にしてください。

■あて先IPアドレス

パケットのIPアドレスを入力します。
ネットワークアドレスを入力することも可能です。
「0/0」または空欄にするとすべてのアドレスを指定したことになります。

■あて先ポート

パケットのあて先ポートまたはサービス名を入力します。
プロトコルがICMPの場合、ICMPコードを指定できます。
「開始ポート:終了ポート」のように範囲を指定できます。
空欄にするとすべてのポートまたはICMPコードを指定したことになります。
プロトコルがGREの場合、あて先ポート指定はありませんので空欄にしてください。

8-4. IPフィルタリングの削除
設定されているフィルタを削除します。

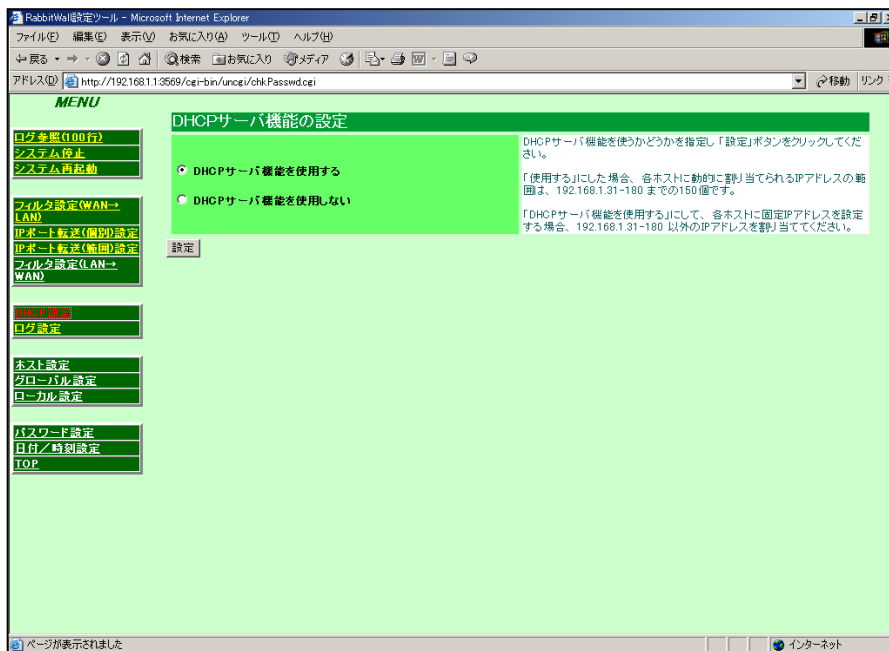
削除	(フィルタの識別番号を選択した後、「削除」ボタンで削除します。)
220 ▼ 削除	

削除したフィルタの設定を再度利用する場合は、「追加」から再度設定して下さい。

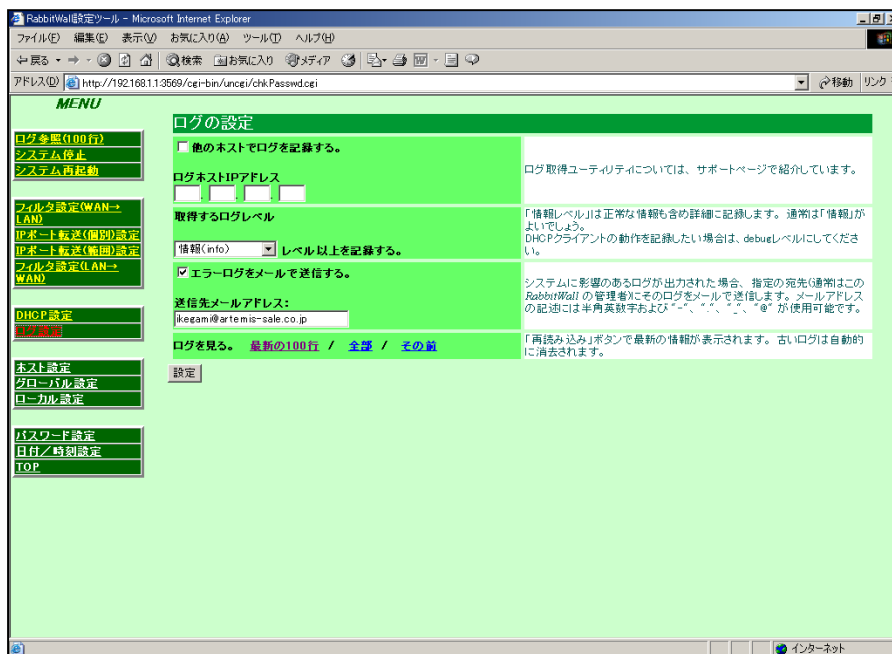
8-5. IPフィルタリングの初期化
フィルタリングの設定を初期状態に戻します。

「デフォルトに戻す」をクリックすると、確認画面が表示されますので、初期状態に戻したい場合は
「はい」をクリッして下さい。

9. DHCP設定

DHCPサーバの起動、停止を設定します。

「使用する」にした場合、各ホストに動的に割り当てられるIPアドレスの範囲は、192.168.0.31～180までの150個です。
「使用する」にして各ホストに固定IPアドレスを設定する場合、192.168.0.31～180以外のIPアドレスを割り当ててください。

10. ログ設定

システムログの出力設定を行います。

10-1. 他のホストでログを記録する

X-Terminator αのシステムログを、他のホストに転送して記録します。

■他のホストでログを記録する

X-Terminator α以外のホストでログを記録する場合はチェックを付けます。

■ログホスト**IP**アドレス

ログを記録したいホストのIPアドレスを入力します。

※syslogによる出力を受信できるホストが必要です。

10-2. 取得するログレベル
ログを記録する範囲を指定します。
「デバッグ」から「エラー」までの5段階があり、段階が上がるにつれて、出力するログの量は少なくなります。

■デバッグ（debug）

■情報（info）

■注意（notice）

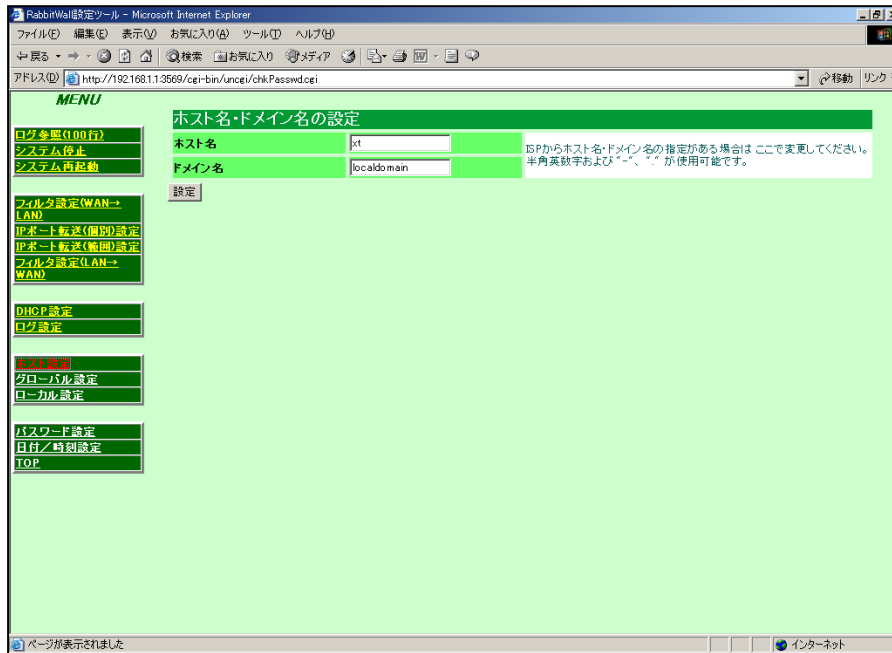
■警告（warning）

■エラー（error）

10-3. エラーログをメールで送信する
システムに影響のあるログが出力された場合、指定の宛先にそのログをメールで送信します

10-4. ログを見る
「最新の100行」、「全部」、「その前」のログを一覧表示します。
「再読み込み」ボタンで最新の情報が表示されます。
古いログは自動的に消去されていきます。

11. ホスト設定

X-Terminator α自体に設定するホスト名、ドメイン名を入力します。

ISPからホスト名、ドメイン名の指定がある場合はここで変更して下さい。

12. グローバル設定

ここではグローバル側のネットワークに関する設定を行います。

12-1. DHCPサーバからの取得

WAN側に接続されているDHCPサーバからIPアドレスを取得します。

DHCPサーバからIPアドレスを取得できなかった場合は「(再取得する)」を押して下さい。
取得したIPアドレスは「取得したIPアドレス:」に表示されます。

12-2. 固定IPアドレス設定

グローバル側のネットワークに固定でIP設定を行います。

固定IPアドレス設定		
IPアドレス	192 . 168 . 0 . 1	IPアドレスを「123.123.123.123」のように入力してください。
サブネットマスク	24/255.255.255.0	サブネットマスクを24のようなビット数か「255.255.255.0」のようなアドレスから選択してください。選択肢は「ビット数/アドレス」のようになっています。
ブロードキャストアドレス	サブネット＋全部1	ブロードキャストアドレスを指定してください。わからない場合は「サブネット＋全部1」を選んでください。
ゲートウェイアドレス	192 . 168 . 0 . 100	ゲートウェイアドレスを「123.123.123.123」のように入力してください。
DNSアドレス	192 . 168 . 0 . 100	DNSのアドレスを「123.123.123.123」のように入力してください。この *RabbitWall* の DHCPサーバ機能を使用する場合に、各ホストにここで設定したDNSアドレスが配られます。最低1つは設定してください。
MACアドレス	00:E0:4C:77:23:6F	接続会社にMACアドレスを申請する場合は、このアドレスを使用します。

設定

各項目に入力を行って「設定」ボタンをクリックして下さい。

■IPアドレス

設定したいIPアドレスを入力して下さい。

■サブネットマスク

設定したいネットマスクを一覧から選択して下さい。

■ブロードキャストアドレス

設定したいブロードキャストアドレスを一覧から選択してください。
わからない場合は「サブネット＋全部１」を選んでください。

■ゲートウェイアドレス

X-Terminator αにとってのゲートウェイアドレスを入力してください。

■DNSアドレス

DNSのアドレスを入力してください。DHCPサーバ機能を使用する場合は、ここで設定したDNSアドレスが各クライアントに対して配られますので、最低１つは設定してください。

■MACアドレス

接続会社にMACアドレスを申請する場合は、このアドレスを使用します。
　　※変更は出来ません

12-3. ADSL設定

ADSL接続（PPPoE）の設定を行います。

ADSL設定		
ユーザ名	username	プロバイダから指示されているユーザ名を入力して下さい。
パスワード	********	プロバイダから指示されているパスワードを入力して下さい。
再接続(分)	6	通信が指定時間(分)以上途絶えたとき、自動的に接続を再起動します。通常は変更の必要はありません。
DNSアドレス		PPPoE接続時に使用するDNSのアドレスを「123.123.123.123」のように指定します。通常は、接続時に局から配布されますので設定不要です(配布されたDNSアドレスが表示されます)。指定した場合、*RabbitWall* のDHCPサーバ機能を使用する場合に各パソコンにこのDNSアドレスが配られます。

■ユーザ名

プロバイダから指示されているユーザ名を入力して下さい。

■パスワード

プロバイダから指示されているパスワードを入力して下さい。

■再接続(分)

通信が指定時間(分)以上途絶えたとき、自動的に接続を再起動します。

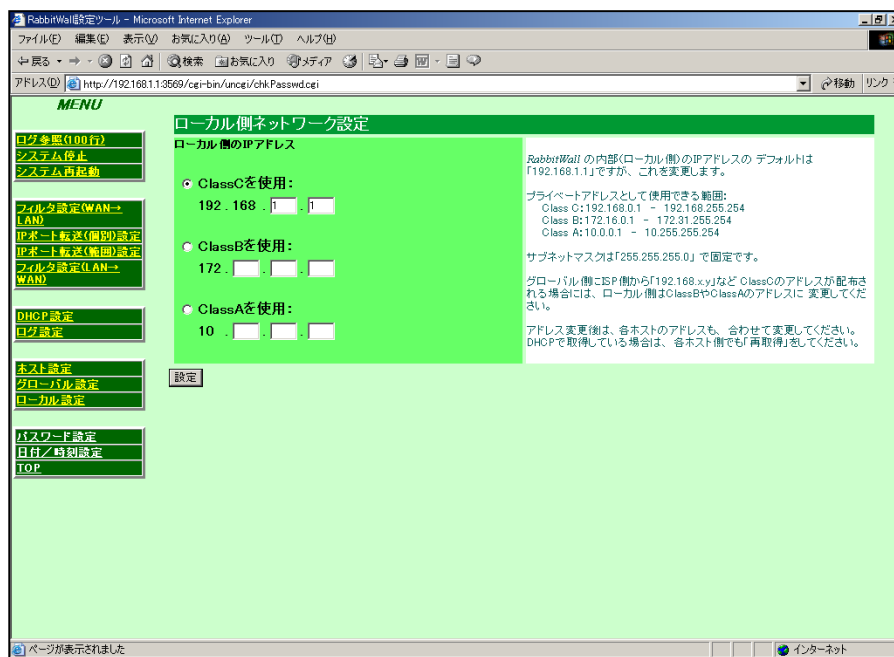
通常は、変更の必要はありません。

■DNSアドレス

PPPoE接続時に使用するDNSのアドレスを入力します。

通常は、接続時に局から配布されますので設定不要です。
(配布されたDNSアドレスが表示されます)

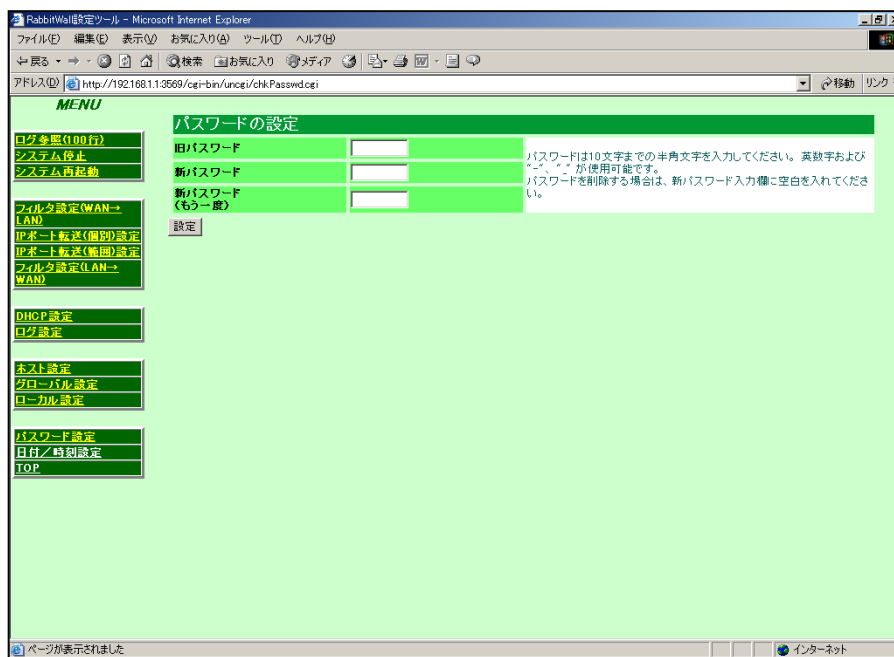
13. ローカル設定

LAN側（ローカル側）のIPアドレスを変更する際に使用します。

ローカル側のアドレスとして使用できる範囲は以下の通りです。

■タイプC192.168.0.1　～　192.168.255.254
■タイプB172.16.0.1　～　172.31.255.254
■タイプA10.0.0.1　～　10.255.255.254
■サブネットマスクは「255.255.255.0」で固定です。

アドレス変更後は、各クライアントのアドレスも合わせて変更して下さい。
DHCPで取得している場合は、各クライアント側でも再取得の作業を行って下さい。

14. パスワード設定

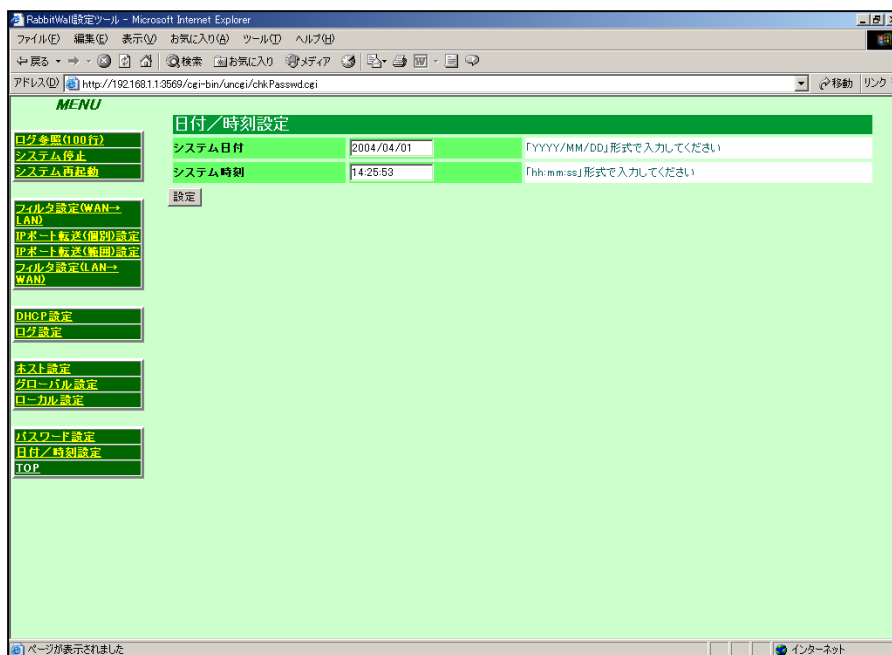
設定画面に入る際のパスワードを変更します。

■旧パスワード

現在のパスワードを入力します。

■新パスワード

新しいパスワードを10文字以内で入力して下さい。
「新パスワード」欄に何も入れなかった場合、パスワードは「無し」になります。

15. 日付/時刻設定

日付／時刻の設定を行います。

■システム日付

「YYYY/MM/DD」形式で入力してください。

例） 2002/10/25

■システム時刻

「hh:mm:ss」形式で入力してください。

例） 14:39:45

*Rabbitwall*のメンテナンスメニュー設定

1. メンテナンスメニュー

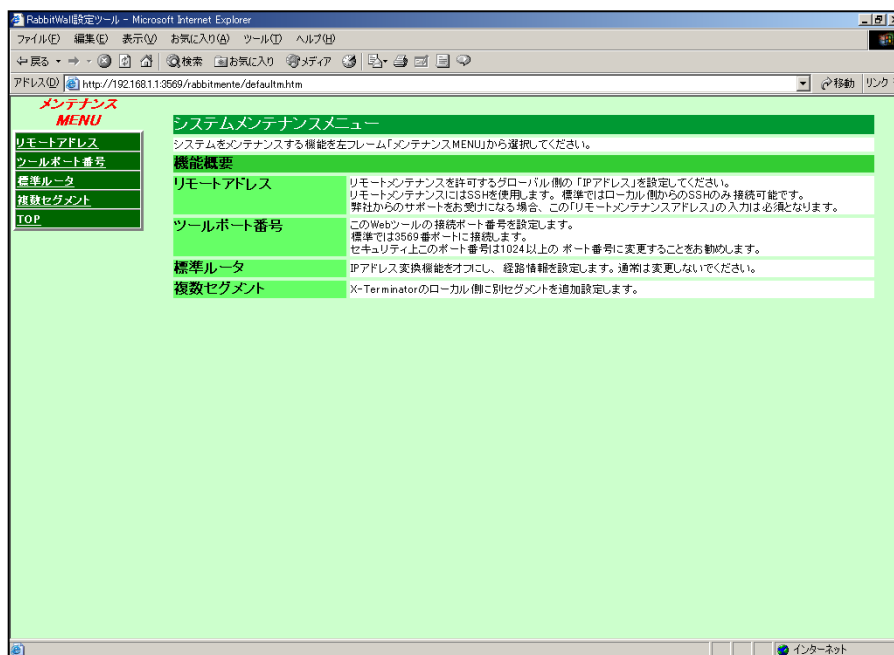
RabbitWallには、通常変更することの少ない項目や、設定を変更することでシステムに大きな影響を与える項目を、通常のメニュー画面から切り離してあります。

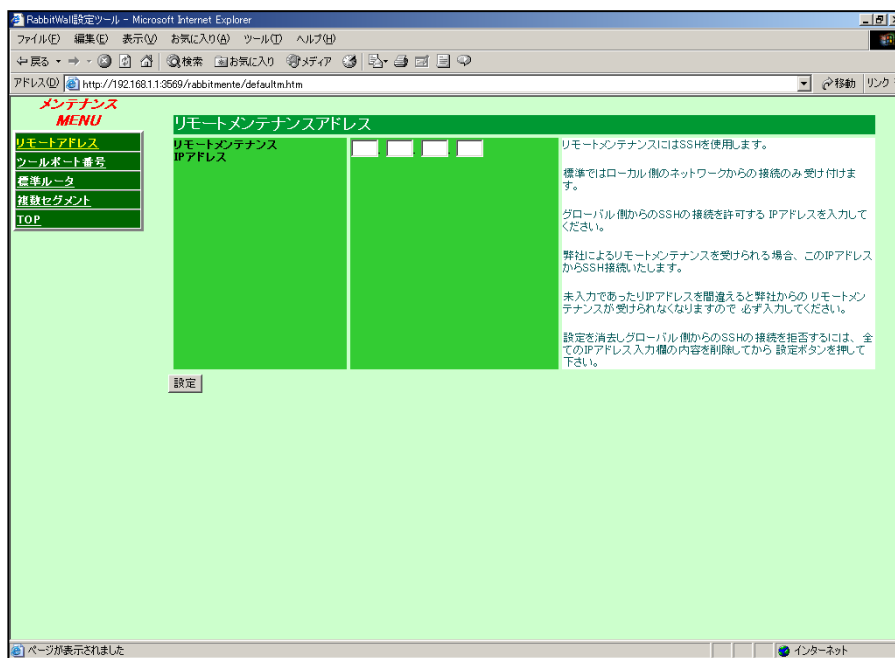
1-1. メンテナンスメニューへのアクセス方法

ブラウザのアドレスバーに
http://192.168.1.1:3569/rabbitmente/defaultm.htm と入力します。

アドレス“http://192.168.1.1:3569/rabbitmente/defaultm.htm”

1-2. *RabbitWall*メンテナンスメニュー

「***RabbitWall***メンテナンスメニュー」という画面が開き、各種設定が行えます。

2. リモートアドレス

リモートメンテナンスを行う際の設定を行います。

リモートメンテナンスにはSSH（暗号化された遠隔管理プロトコル）を使用します。
グローバル側からのSSHの接続を許可するIPアドレスを入力してください。
リモートメンテナンスをする場合、このIPアドレスからリモート接続いたします。

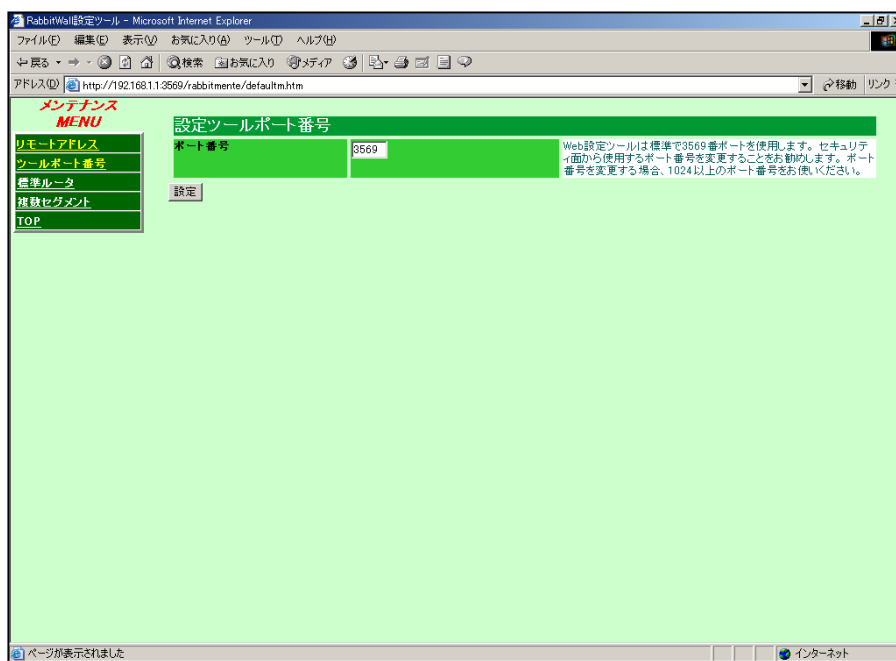
※グローバルIPが固定でない場合でも、その時点のIPを入力すればリモートサポートは可能ですが、IPアドレスの割り当てが変更された時点で通信不能となります。

その場合は再度、適切なIPアドレスに設定を変更する必要があります。
あらかじめご了承ください。

※未入力や誤設定の場合、リモートメンテナンスが受けられませんので、入力ミスのないよう御注意ください。

設定を消去するには、全てのIPアドレス入力欄の内容を削除してから設定ボタンを押して下さい。

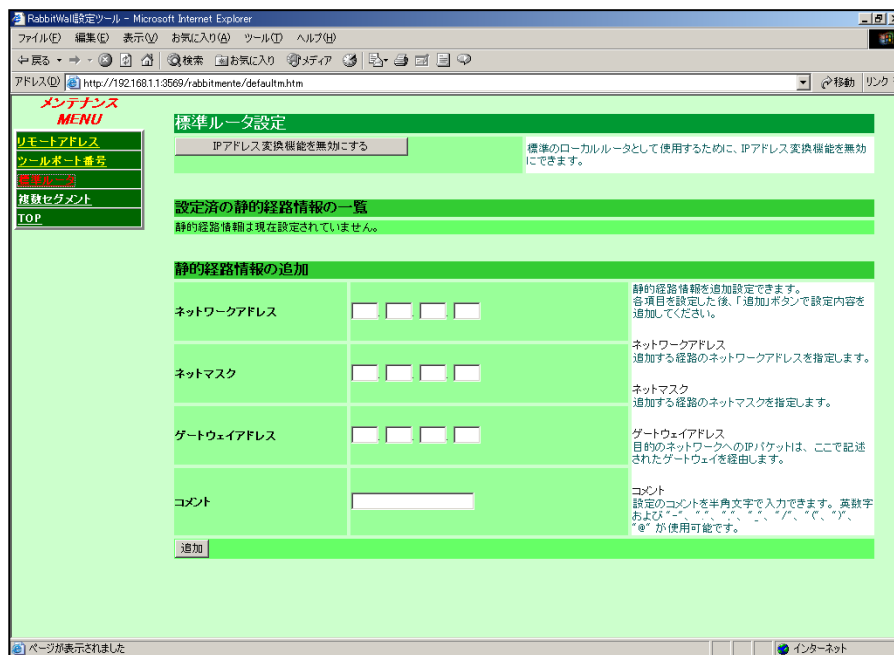
3. ツールポート番号

Web設定ツール画面にアクセスするためのポート番号を変更します。

Web設定ツールは標準で3569番ポートを使用しますが、セキュリティ面から使用するポート番号を変更することをお勧めします。

ポート番号を変更する場合、1024以上のポート番号をお使いください。

4. 標準ルータ

4-1. IPアドレス変換機能の切り替え

外部と内部のIPアドレスをIPマスカレード機能で変換しています。

■IPアドレス変換機能を無効/有効にする

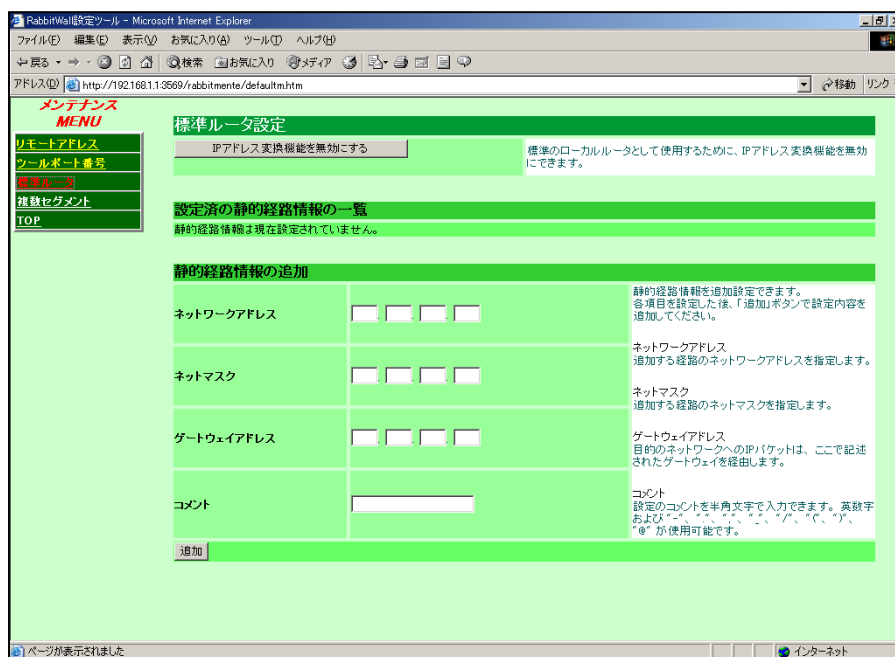
IPマスカレード機能を使用するか使用しないかを切り替えることができます。
ボタン名は現在の状況によって「有効にする（IPマスカレード機能を無効にしている場合の表示）」「無効にする（IPマスカレード機能を有効にしている場合の表示）」と表記が変わります。

IPアドレス変換機能を無効にすることで、ローカルルータと同じように使用することができます。

4-2. 設定済の静的経路情報の一覧

現在設定されている静的経路情報が一覧表示されます。
初期設定の段階では、一切設定が入っていない状態のため、「設定済の静的経路情報は現在設定されていません。」という表示となります。

4-3. 静的経路情報の追加

新規に静的経路情報の設定を追加できます。

追加した設定はそのまま有効になりますので、静的経路情報を一時的に無効にする場合は、「静的経路情報の削除」から設定を無効にして下さい。

■ネットワークアドレス

追加する経路のネットワークアドレスを指定します。

■ネットマスク

追加する経路のネットマスクを指定します。

■ゲートウェイアドレス

目的のネットワークへのIPパケットは、ここで記述されたゲートウェイを経由します。

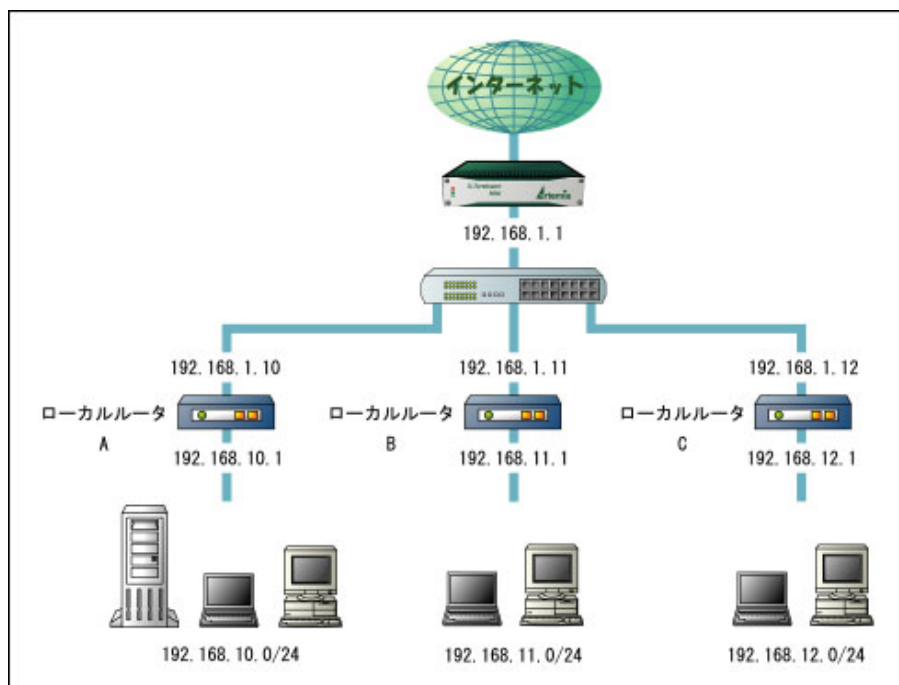
■コメント

設定のコメントを半角文字で入力できます。
半角英数字および - . , _ / ( ) @ が使用可能です。

4-4. 静的経路情報の削除

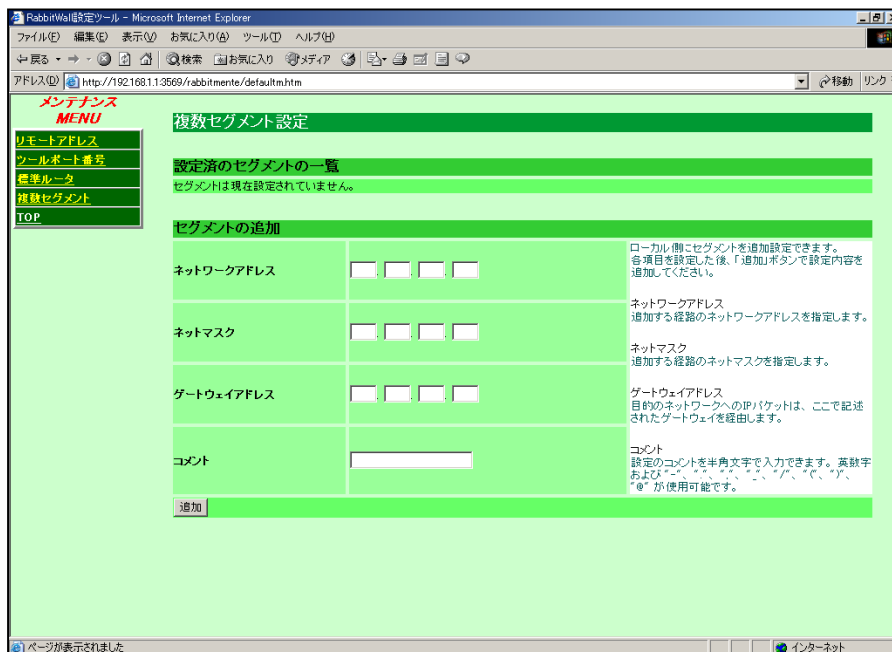
設定されている静的経路情報を削除できます。
削除した静的経路情報を再度利用する場合は、「静的経路情報の追加」から再設定する必要があります。
削除したい静的経路番号を選択して「削除」ボタンをクリックして下さい。

5. 複数セグメント設定

下記のような、ローカルルータを使用してセグメントを複数使用しているネットワークに接続する場合、各ローカルルータの下部にあるネットワークの設定を追加する事により、外部へ接続できるように設定します。

5-1. 設定済のセグメントの一覧

現在設定されているセグメント情報が一覧表示されます。
表示されている項目が現在有効になっている設定です。
初期設定の段階では、一切設定が入っていない状態のため、「セグメントは現在設定されていません。」という表示となります。

5-2. セグメントの追加

新規にセグメントの設定を追加できます。

内容を記入して「追加」ボタンをクリックすると、セグメントの設定が追加されます。
追加した設定を有効にするには再起動を行ってください。
設定を一時的に無効にする場合は、「セグメントの削除」から設定を削除して下さい。

■ネットワークアドレス

追加する経路のネットワークアドレスを指定します。

■ネットマスク

追加する経路のネットマスクを指定します。

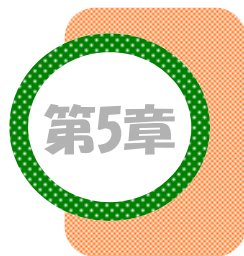
■ゲートウェイアドレス

目的のネットワークへのIPパケットは、ここで記述されたゲートウェイを経由します。

■コメント

設定のコメントを半角文字で入力できます。
半角英数字および - . , _ / ( ) @ が使用可能です。

5-3. セグメントの削除

設定されているセグメントを削除できます。
削除したセグメントを再度利用する場合は、「セグメントの追加」から再設定する必要があります。

*Rabbitwall*の保守メニュー　設定

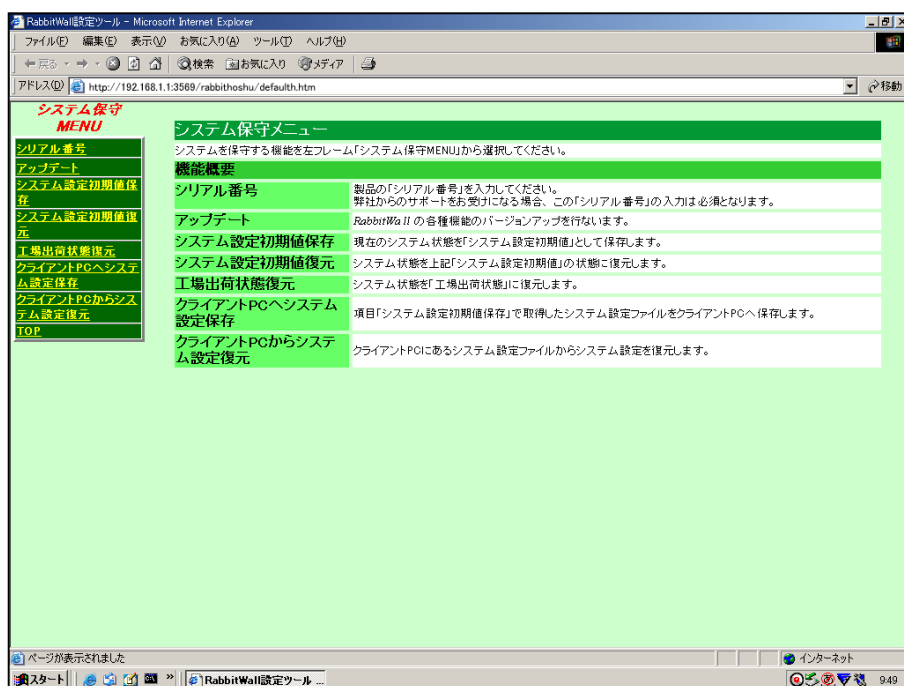
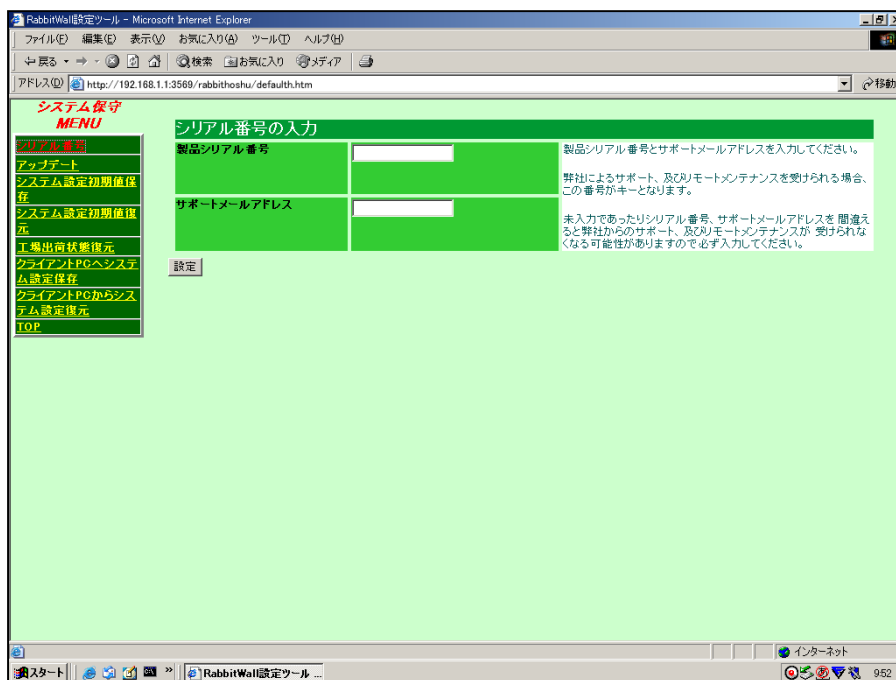
1. システム保守メニュー

1-1. システム保守メニューへのアクセス方法

ブラウザのアドレスバーに
http://192.168.1.1:3569/rabbithoshu/defaulth.htm と入力します。

アドレス“ **http://192.168.1.1:3569/rabbithoshu/defaulth.htm** ”

1-2. システム保守メニュー

「***RabbitWall***メンテナンスメニュー」という画面が開き、各種設定が行えます。

2. シリアル番号の入力

製品の「シリアル番号」を入力してください。

■製品シリアル番号

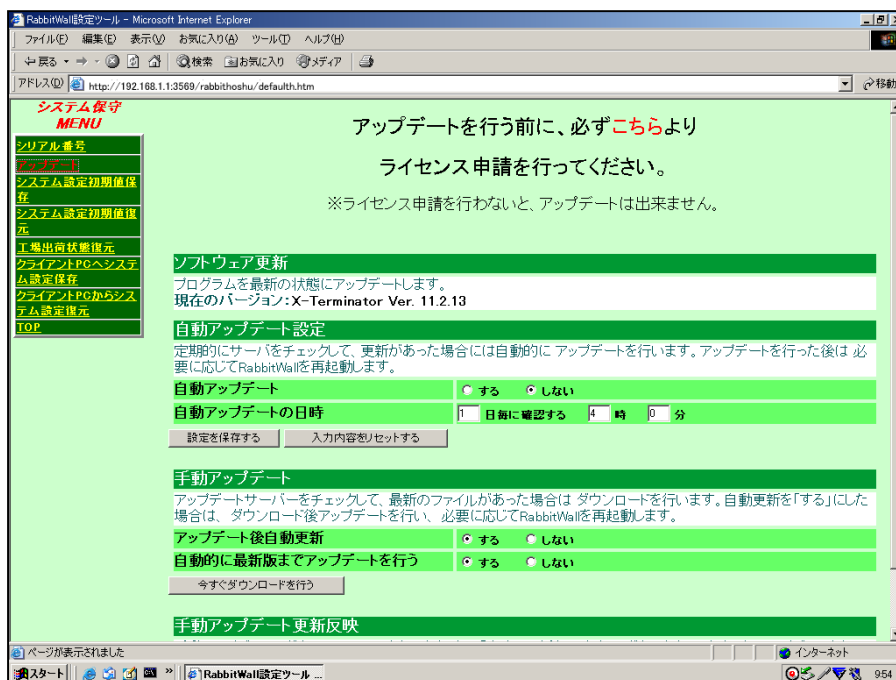
*X-Terminator α*のシリアルナンバー（本体底面に刻印されています）

■サポートメールアドレス

サポート業者様のメールアドレスを入力してください。
自動アップデートサービスなどを受けられる場合、このシリアル番号がキーとなります。

※未入力や誤登録の場合、自動アップデートサービスなどが受けられませんので、入力ミスのないよう御注意ください。

3. アップデート

RabbitWallのプログラムを最新のものにアップデートすることができます。

※アップデートを行う前に、必ずこちらよりライセンス申請を行ってください。
ライセンス申請を行わないと、アップデートは出来ません。

3-1. 自動アップデート設定

自動アップデートの設定を行います。

■自動アップデート

自動アップデートを行うかどうかを選択します。

■アップデートの日時

サーバへ更新ファイルの確認をする日時)を入力します。

※自動、手動アップデートを行う場合には、別途保守契約が必要となります。

3-2. 手動アップデート

手動でアップデートを行う場合の設定をします。

手動アップデート	
アップデートサーバーをチェックして、最新のファイルがあった場合は ダウンロードを行います。自動更新を「する」にした場合は、ダウンロード後アップデートを行い、必要に応じてRabbitWallを再起動します。	
アップデート後自動更新	○ する ◉ しない
自動的に最新版までアップデートを行う	○ する ◉ しない
今すぐダウンロードを行う	
手動アップデート更新反映	
手動アップデートでダウンロードのみを行った場合、「今すぐ更新を反映する」ボタンをクリックすると アップデートを行い、必要に応じてRabbitWallを再起動します。	
今すぐ更新を反映する	

■アップデート後自動更新

アップデート後に自動で再起動するかどうかを選択します。
（しないを選択した場合、手動で再起動を行う事によりアップデートが終了します）

■自動的に最新版までアップデートを行う

更新内容が複数あった場合、最新版までアップデートを繰り返します。

■今すぐ更新を反映する

「アップデート後自動更新」を“しない”に設定した場合、このボタンを押す事でアップデートした内容が更新されます。

■手動アップデート時のメッセージ一覧

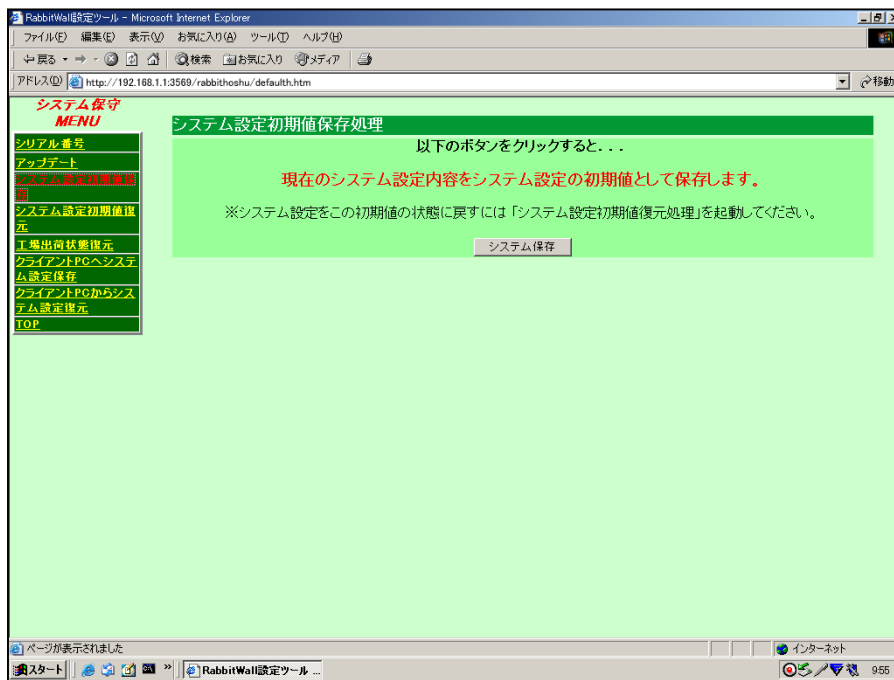
メッセージ	状態	詳細
アップデートサーバに接続しています	サーバに接続中	アップデートサーバに接続中
接続に失敗しました	接続失敗	アップデートサーバに接続できませんでした
データをダウンロードしています	ダウンロード中	アップデートファイルのダウンロード中です
ダウンロードが成功しました	ダウンロード成功	アップデートファイルのダウンロードが完了しました
ダウンロードが失敗しました	ダウンロード失敗	アップデートファイルのダウンロードに失敗しました
更新を反映しています	アップデート後自動更新（する）	アップデートファイルをシステムに反映しています
「今すぐ更新を反映する」ボタンをクリックするとアップデートされます	アップデート後自動更新（しない）	
更新を反映しています	設定反映中	アップデート処理中です
アップデートが成功しました	更新成功	アップデート処理が完了しました
アップデートが失敗しました	更新失敗	アップデート処理が途中で中断されました
シリアル番号を入力してください	シリアル番号空白	シリアル番号が入力されていません
こちらからライセンス申請を行った後、再度アップデートを行ってください。	シリアル番号未登録	アップデートサーバに未登録のシリアル番号です
保守契約がされていません	保守契約なし	アップデートサーバに保守契約情報が登録されていません
更新の必要はありません	最新のバージョン	現在のバージョンが最新バージョンです
サーバはメンテナンス中です	サーバが拒否	アップデートサーバがメンテナンス中です

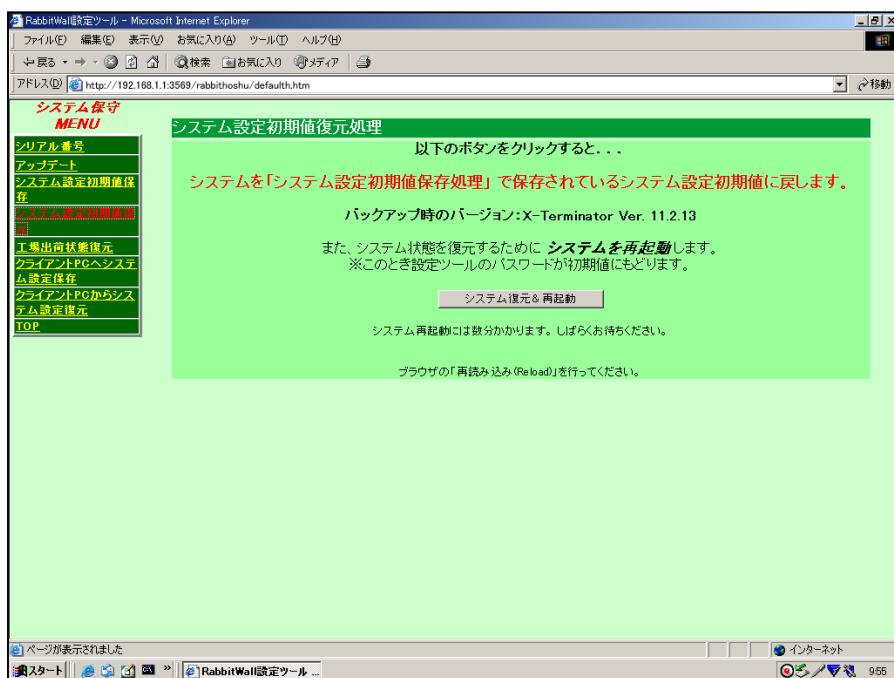
3-3. アップデートファイルによるソフトウェア更新

本機能は通常使用しません。

※弊社（委託業者を含む）技術者によるメンテナンス時に利用します。

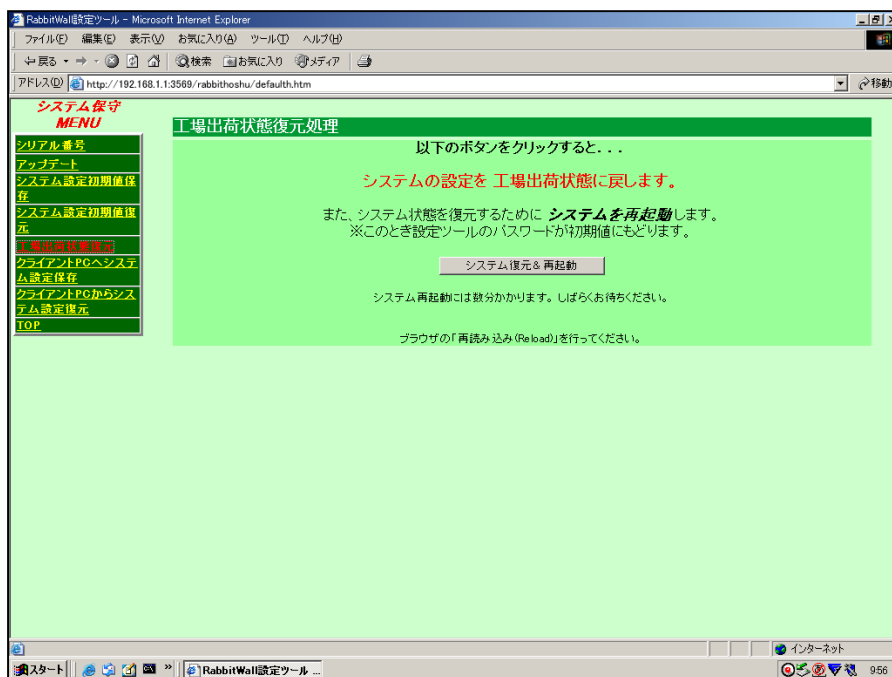
4. システム設定初期値保存

現在のシステム設定内容をシステム設定の初期値として保存します。

5. システム設定初期値復元

システムを「システム設定初期値保存」で保存した状態に戻します。

「システム復元＆再起動」ボタンを押すと現在の設定が保存され、*X-Terminator α*が再起動します。

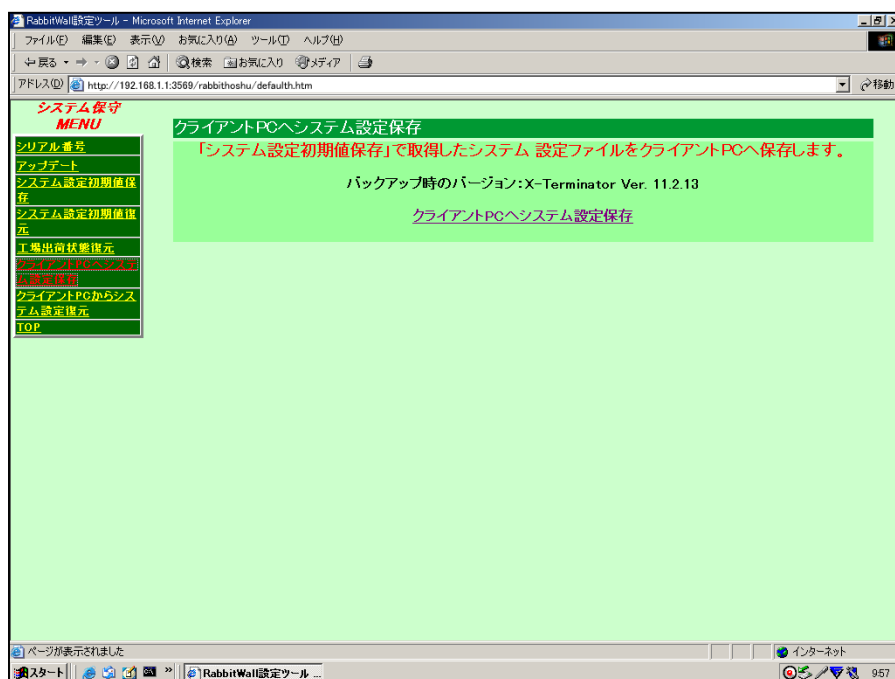
この際、システム状態を復元するために*X-Terminator α*を再起動します。
再起動完了後、ブラウザの「更新(Reload)」を行ってください。

6. 工場出荷状態復元

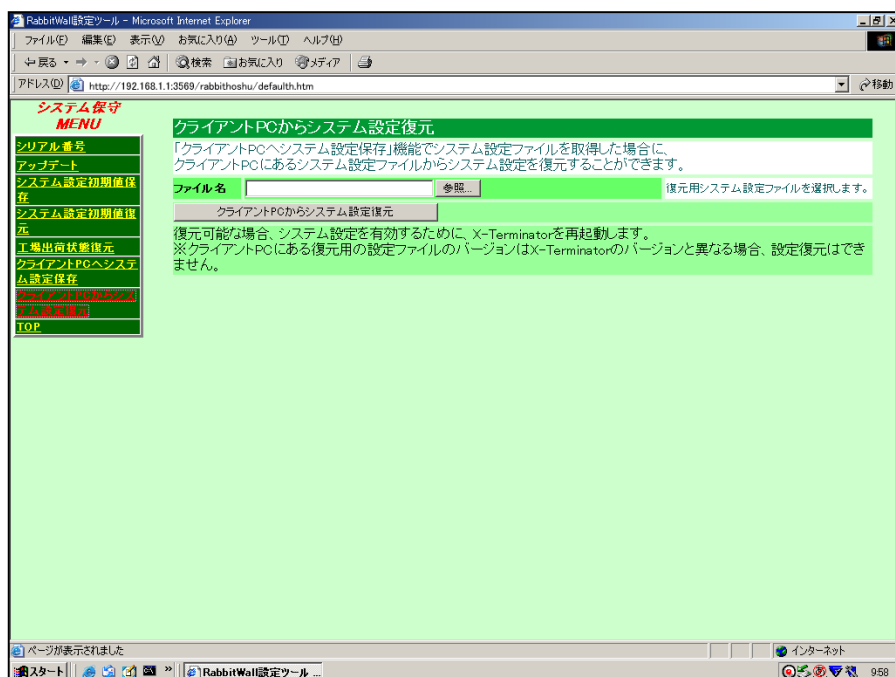
システムの設定を工場出荷状態に戻します。

「システム復元＆再起動」ボタンを押すと現在の設定が保存され、***X-Terminator α***が再起動します。
この際、システム状態を復元するために***X-Terminator α***を再起動します。

このとき設定ツールのパスワードが初期値“rabbit”に戻ります。
再起動完了後、ブラウザの「更新(Reload)」を行ってください。

7. クライアントPCへシステム設定保存

「システム設定初期値保存」(57P)で取得したシステム 設定ファイルをクライアントPCへ保存します。

※クライアントPCに保存する前に、バックアップ時のバージョンを確認し、最新のバージョンではない場合は、システム初期値を再度保存して、最新の状態にして下さい。

8. クライアントPCからシステム設定復元

「クライアントPCへシステム設定保存」機能でシステム設定ファイルを取得した場合に、
クライアントPCにあるシステム設定ファイルからシステム設定を復元することができます。

復元可能な場合、システム設定を有効するために、***X-Terminator α***を再起動します。

※クライアントPCにある復元用の設定ファイルのバージョンが、復元に使用する
X-Terminator αのバージョンと異なる場合、設定復元はできません。
※***X-Terminator***シリーズの復元用設定ファイルは、***X-Terminator α***シリーズにおいて
設定復元することはできません。

アンチウイルス(旧*X-Wall*)設定メニュー

ウイルスソフト **ver2.xx** までは***X-Wall***と表示されます。

ウイルスソフト **ver3.xx** からは**F-Secure**アンチウイルス**Linux**ゲートウェイと表示されます。ウイルス検査エンジンの変更、画面やデザイン、カラーを一新しました。

1. アンチウイルス設定メニューへのアクセス方法

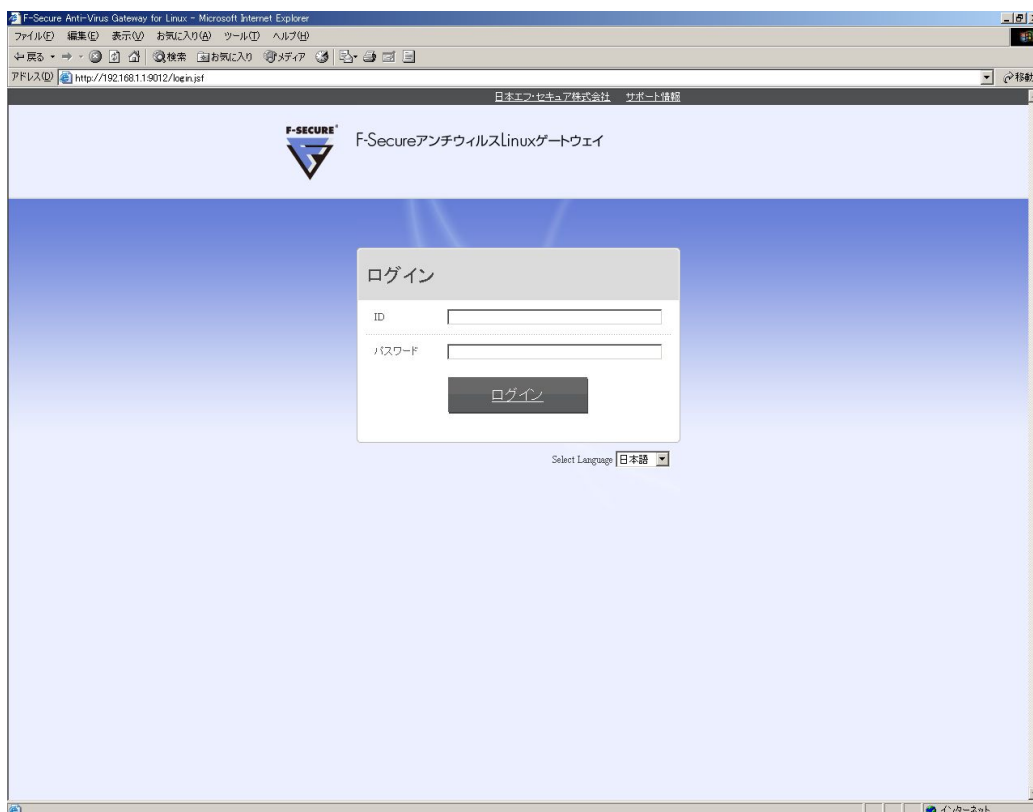
1-1.アンチウイルス設定メニューへのアクセス方法

ブラウザアドレスバーに“192.168.1.1:9012”と入力します。

アドレス　“http://192.168.1.1:9012”

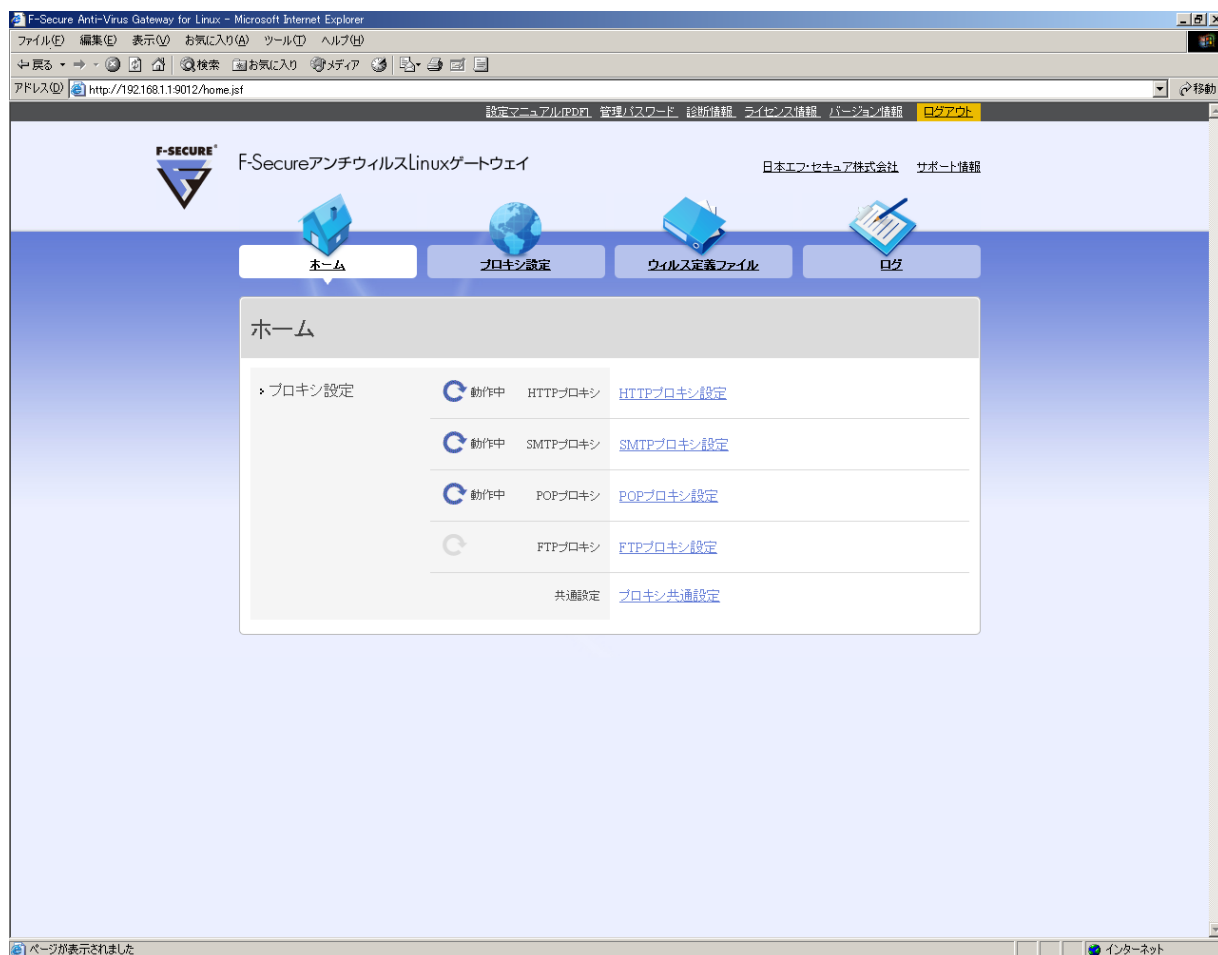
1-2.アンチウイルス設定メニューへのログイン方法

ユーザー名 ”admin”、パスワード ”admin”と入力します。
ログインをクリックしてください。　［Enter］キーではログインできません。

ユーザ名“admin”、パスワード“admin”

1-3. アンチウイルス設定メニュー

メイン画面が表示されます。ここから各種設定を行います。

ウイルスソフト Ver３.xx からは「F-SecureアンチウイルスLinuxゲートウェイ」と表示され、Ver２.xx までの「*X-Wall*」　に表示がなかった機能につきましては、原則 動作保証対象外 となりますので、ご使用にならない様にお願い申し上げます。

※FTPプロキシ設定は動作保証対象外となりますので設定しないでください。

2. プロキシ設定

アンチウイルスLinuxゲートウェイはウィルススキャンを行なうプロキシサービスです。
『手動プロキシ』モードと『透過プロキシモード』と呼ばれる二つのモードで運用されます。

『手動プロキシモード』
プロキシサービスに関する設定を任意に行なうことができます。
※こちらは、アンチウイルスの設定に加え、クライアント側[ブラウザ,メーラー]の設定も必須になります。

『透過プロキシモード』
クライアント側の設定を透過的に利用し処理を行います。
この為、ここのクライアント設定に柔軟に合わせる事が可能です。
※こちらの設定では、プロキシサービスの「NATリダイレクト」設定が必要不可欠になります。

2-1. HTTPプロキシ

HTTPプロキシサービスの有効・無効を設定します。
※設定後に画面一番下の「保存・再起動」ボタンをクリックすることにより設定が反映されます。

■ポート番号
　プロキシサービスのポート番号を指定します。
※必要の際には、任意のポート番号に変更することができます。

■親サーバ
　上部にHTTPプロキシサーバなどがあり接続の必要がある場合、IPアドレスもしくはホスト名を入力
　します。
※「透過プロキシ」設定を有効化している場合は、この設定は無効化されます。(クライアントの設定を透過的に利用します。)

■ウイルス検査
　ウイルス検査の有無を指定します。※通常はチェックします。

ウイルス検出時の動作	削除 管理者へメールで通知 ※通知先は、[共通設定] の [管理者への通知設定] で設定できます。 隔離保存 ※隔離先は、[共通設定] の [隔離保存ディレクトリ] で設定できます。 検出メッセージの編集
プロキシ認証	有効 無効 ユーザ情報の編集
最大同時接続数	10
アクセス制御 指定したホスト一覧からの接続のみ受け付けます。	接続元 ※「DNS逆引き」を有効にするとホスト名・ドメイン名での指定も可能になります。 ※複数指定をする際は、指定ごとに改行入力してください。 ※最大で1999バイトまで設定できます。 接続先 ※複数指定をする際は、指定ごとに改行入力してください。 ※最大で1999バイトまで設定できます。

■ウイルス検出時の動作

・削除：ウイルスを削除します。※通常はチェックします。

・管理者へメールで通知：ウイルス感染情報を指定したアドレスにメールで通知します。

・隔離保存： 動作保証対象外となりますので設定しないでください。

・検出メッセージ：ウイルス検出時に表示するメッセージを編集することができます。
（日本語での設定が可能です）

■プロキシ認証

動作保証対象外となりますので設定しないでください。

■最大同時接続数

接続数を増やすことにより、クライアントへのレスポンスが上がります。

※数を増やしすぎると、メモリを多く消費するため筐体能力を考慮し設定してください。出荷時は「50」に設定されています。

■アクセス制御

動作保証対象外となりますので設定しないでください。

■検査除外対象

・User-Agent：指定したUser-Agentを持つ接続の場合は、検査を行いません。

※複数指定をする際は、指定ごとに改行入力してください。
また前方一致で検索します。

・ホスト名：検査を行なわないホストを記述します。

・ファイル名/拡張子：ウイルス検査を行なわないファイルや拡張子を指定します。

・ファイルサイズ：動作保証対象外となりますので設定しないでください。

■DNS逆引き

動作保証対象外となりますので設定しないでください。

■最大検査時間

動作保証対象外となりますので設定しないでください。

■ファイルアップロード時のウイルス検査

動作保証対象外となりますので設定しないでください。

■リスクウェア検査

動作保証対象外となりますので設定しないでください。

■keep-Alive接続

動作保証対象外となりますので設定しないでください。

■匿名プロキシモード

動作保証対象外となりますので設定しないでください。

■透過プロキシモード【NAT（iptables）リダイレクト設定】

透過プロキシを有効にします。
動作させる場合、先にNAT設定画面からNATのリダイレクト設定が必要になります。
（NATリダイレクト設定は79P）

■エラーメッセージ

動作保証対象外となりますので設定しないでください。

2-2. SMTPプロキシ

SMTPプロキシサービスの有効・無効を設定します。

※設定後に画面一番下の「保存・再起動」ボタンをクリックすることにより設定が反映されます。

■ポート番号
プロキシサービスのポート番号を指定します。

※必要の際には、任意のポート番号に変更することができます。

■ウイルス検査
ウイルス検査の有無を指定します。

■親サーバ
メールの転送を依頼したいSMTPサーバのホスト名・ポート番号を指定します。

※「透過プロキシ」設定を有効化している場合は、この設定は無効化されます。
(メールクライアントで設定しているメールサーバアドレスへメール転送を行なう為)

■全体設定
ウイルス検出時の動作

- ･通過：ウイルスを発見しても何もしない。
  ※通常は設定しません。
- ･送信拒否：ウイルス検出メールの送信を拒否し、メーラやメールサーバに直接通知します。
- ･削除：ウイルスを削除しますが、検出メッセージは送信しません。
- ･削除後、受信者へ通知：ウイルスを削除して、検出メッセージをメールで受信者に送付します。
- ･削除後、送信者へ通知：ウイルスを削除し、検出メッセージをメールで送信者に送付します。
  ※送信者は偽造が可能な為、通常利用しません。
- ･管理者へ通知：ウイルス感染情報を指定したアドレスにメールで通知します。
- ･隔離保存： 動作保証対象外となりますので設定しないでください。
- ･検出メッセージの編集：ウイルス検出時に表示するメッセージを編集することができます。
  （日本語での設定が可能です）

■スパム検査

共通設定内のスパム認知条件に基づき、スパムメールであることが分かる目印をつける機能です。

目印付きのメールに対して、メールソフトにて振り分け条件を作ることにより、スパムメールの取り扱いを管理しやすくします。

※通常のメールがスパムメールとして判定されてしまう場合もあるため、削除する前に確認するようにして下さい。

・通過：(X-Spam-Status付加のみ)スパムを通過します。
　スパムと判定されたメールは、ヘッダに"X-Spam-Status"が付加されます。クライアントの振り分け設定を利用してスパムメールとして振り分けを行い、メールの管理をしやすくします。

・件名変更(追加文字列)：スパムと判定したメールの件名を変更します。
　「追加文字列」で指定した文字列を件名の先頭に付加します。

・削除：スパムと判定したメールを削除します。

・隔離保存：動作保証対象外となりますので設定しないでください。
・管理者へメールで通知：スパムメール情報を指定したアドレスにメールで通知します。

■受信先（RPCT）ドメインの制限

動作保証対象外となりますので設定しないでください。

■SMTP認証

動作保証対象外となりますので設定しないでください。

■POP before SMTP認証

動作保証対象外となりますので設定しないでください。

LAN設定 LAN内のホスト/ネットワークからの接続に対して別の動作を指定します。		有効 無効
	LAN内のホスト/ネットワーク	※「DNS逆引き」を有効にするとホスト名・ドメイン名での指定も可能になります。 ※複数指定をする際は、指定ごとに改行入力してください。 ※最大で1999バイトまで設定できます。
	親サーバ	有効 無効 ※無効にした場合、全体設定で指定した内容になります。 ホスト名 ポート番号 25
	ウイルス検出時の動作	通過 ※ログへの記録・管理者通知・ヘッダへのX-Virus-Status:の付加は行います。 送信拒否 ※メーラやメールサーバにSMTPコマンドのエラー応答として直接通知します。 削除 ※メールを削除して通知は行いません。 削除後、受信者へメールで通知 ※ウイルスメールの受信者は詐称されている場合があります。 外部へのメールを処理する場合は、受信者への通知は行わないでください。 削除後、送信者へメールで通知 ※ウイルスメールの送信者は詐称されている場合があります。 外部へのメールを処理する場合は、送信者への通知は行わないでください。 管理者へメールで通知 ※通知先は、[共通設定] の [管理者への通知設定] で設定できます。 隔離保存 ※隔離先は、[共通設定] の[隔離保存ディレクトリ] で設定できます。 検出メッセージの編集
最大同時接続数		10

■LAN設定

動作保証対象外となりますので設定しないでください。

■最大同時接続数

接続数を増やすことにより、クライアントへのレスポンスが上がります。
※数を増やしすぎると、メモリを多く消費するため筐体能力を考慮し設定してください。
出荷時の設定は、Mini α10、Appliance α25になっております。

■アクセス制御

動作保証対象外となりますので設定しないでください。

■DNS逆引き

動作保証対象外となりますので設定しないでください。

■拒否対象メール

・ActiveX：ActiveXが埋め込まれたHTMLメールを拒否します。

・スクリプト：スクリプト(JavaScript、VBScript等)を含むHTMLメールを拒否します。

・分割メール：動作保証対象外となりますので設定しないでください。

・暗号化書庫ファイル：暗号化書庫ファイル(ZIP、RAR)を含むメールを拒否します。

・ファイル名/拡張子：指定したファイル名、拡張子の添付ファイルを含むメールを拒否します。（.COM、.EXE、.BAT）

検査除外対象	ファイル名/拡張子 ※複数指定をする際は、指定ごとに改行入力してください。 ※最大で1999バイトまで設定できます。
最大検査時間	90 秒 ※0秒に指定した場合は、時間制限なしとなります。 また、指定数値を0や大きくした場合検査に時間がかかり、 プロキシ処理が停止する恐れがあります。
リスクウェア検査	有効 無効 除外リスクウェア ※複数指定をする際は、指定ごとに改行入力してください。 ※最大で1999バイトまで設定できます。
テキスト本文の検査	有効 無効
HTML全体の検査	有効 無効
匿名プロキシ プロキシでヘッダ情報 (Receivedヘッダ) を追加しません。	有効 無効
透過プロキシモード	有効 無効 NAT(iptables)リダイレクト設定

保存・再起動　キャンセル

■検査除外対象
指定したファイル、拡張子に対してはウイルス検査を行いません。

■最大検査時間：動作保証対象外となりますので設定しないでください。
■リスクウェア検査：動作保証対象外となりますので設定しないでください。
■テキスト本文の検査：動作保証対象外となりますので設定しないでください。
■HTML全体の検査：動作保証対象外となりますので設定しないでください。
■匿名プロキシ：動作保証対象外となりますので設定しないでください。

■透過プロキシモード【NAT（iptables）リダイレクト設定】
透過プロキシを有効にします。
動作させる場合、先にNAT設定画面からNATのリダイレクト設定が必要になります。
（NATリダイレクト設定は79P）

2-3. POPプロキシ

POPプロキシ

有効 無効

ポート番号	9110 ※通常は、110を入力
親サーバ	ホスト名 localhost ポート番号 110
ウイルス検査	有効 無効
ウイルス検出時の動作	削除 ※ウイルスを含まれるメールは、検出メッセージで指定した内容になります。 管理者へメールで通知 ※通知先は、[共通設定] の [管理者への通知設定] で設定できます。 隔離保存 ※隔離先は、[共通設定] の [隔離保存ディレクトリ] で設定できます。 検出メッセージの編集

POPプロキシサービスの有効・無効を設定します。

※設定後に画面一番下の「保存・再起動」ボタンをクリックすることにより設定が反映されます。

■ポート番号

プロキシサービスのポート番号を指定します。

※必要の際には、任意のポート番号に変更することができます。

■親サーバ

メールの取得を依頼したいPOPサーバのホスト名・ポート番号を指定します。

※「透過プロキシ」設定を有効化している場合は、この設定は無効化されます。
(メールクライアントで設定しているメールサーバアドレスへメール取得を行なう為)

■ウイルス検査

ウイルス検査の有無を指定します。

■ウイルス検出時の動作

・削除：ウイルスを削除します。通常はチェックします。

・管理者へメールで通知：ウイルス感染情報を管理者のメールアドレスで指定したアドレスにメールで通知します。

・隔離保存： 動作保証対象外となりますので設定しないでください。

・検出メッセージの編集：ウイルス検出時に表示するメッセージを編集することができます。
（日本語での指定が可能です。）

› スパム検査 スパム検査方法は [共通設定] の [スパム検査方法] で設定できます。	有効 無効 通過 ※ログへの記録・管理者通知・ヘッダへのX-Virus-Status:の付加は行います。 件名変更　追加文字列 [[SPAM]] ※最大で99バイトまで設定できます。 管理者へメールで通知 通知先は、[共通設定] の [管理者への通知設定] で設定できます。 隔離保存 ※隔離先は、[共通設定] の [隔離保存ディレクトリ] で設定できます。
› 親サーバのユーザによる指定 (POPユーザ名: user@host)	有効 無効
› POPユーザ制限	有効 無効 ユーザ情報の編集
› 最大同時接続数	10

■スパム検査

共通設定内のスパム認知条件に基づき、スパムメールであることが分かる目印をつける機能です。

目印付きのメールに対して、メールソフトにて振り分け条件を作ることにより、スパムメールの取り扱いを管理しやすくします。

※通常のメールがスパムメールとして判定されてしまう場合もあるため、削除する前に確認するようにして下さい。

・通過：(X-Spam-Status付加のみ)スパムを通過します。
　スパムと判定されたメールは、ヘッダに“X-Spam-Status”が付加されます。クライアントの振り分け設定を利用してスパムメールとして振り分けを行い、メールの管理をしやすくします。

・件名変更(追加文字列)：スパムと判定したメールの件名を変更します。
　「追加文字列」で指定した文字列を件名の先頭に付加し明示的に分かりやすくします。

・管理者へメールで通知：スパムメール情報を指定したアドレスにメールで通知します。

・隔離保存：動作保証対象外となりますので設定しないでください。

■親サーバのユーザによる指定

メーラのユーザ名に“ユーザ名@POPサーバ名”と指定する事でPOPサーバをユーザが指定可能にします。

■POPユーザ制限

動作保証対象外となりますので設定しないでください。

■最大同時接続数

接続数を増やすことにより、クライアントへのレスポンスが上がります。

※数を増やしすぎると、メモリを多く消費するため能力を考慮し設定してください。
出荷時の設定は、Mini α10、Appliance α25になっております。

■アクセス制御

動作保証対象外となりますので設定しないでください。

■DNS逆引き

動作保証対象外となりますので設定しないでください。

■拒否対象メール

･ActiveX：ActiveXが埋め込まれたHTMLメールを拒否します。

･スクリプト：スクリプト(JavaScript、VBScript等)を含むHTMLメールを拒否します。

･分割メール：動作保証対象外となりますので設定しないでください。

･暗号化書庫ファイル：暗号化書庫ファイル(ZIP、RAR)を含むメールを拒否します。

･ファイル名/拡張子：指定したファイル名、拡張子の添付ファイルを含むメールを拒否します。（.COM、.EXE、.BAT）

検査除外対象	ファイル名/拡張子 ※複数指定をする際は、指定ごとに改行入力してください。 ※最大で1999バイトまで設定できます。
最大検査時間	90 秒 ※0秒に指定した場合は、時間制限なしとなります。 また、指定数値を0や大きくした場合検査に時間がかかり プロキシ処理が停止する恐れがあります。
リスクウェア検査	有効 無効 除外リスクウェア ※複数指定をする際は、指定ごとに改行入力してください。 ※最大で1999バイトまで設定できます。
テキスト本文の検査	有効 無効
HTML全体の検査	有効 無効
透過プロキシモード	有効 無効 NAT(iptables)リダイレクト設定

保存・再起動　キャンセル

■検査除外対象
指定したファイル、拡張子に対してはウイルス検査を行いません。

■最大検査時間：動作保証対象外となりますので設定しないでください。
■リスクウェア検査：動作保証対象外となりますので設定しないでください。
■テキスト本文の検査：動作保証対象外となりますので設定しないでください。
■HTML全体の検査：動作保証対象外となりますので設定しないでください。

■透過プロキシモード【NAT（iptables）リダイレクト設定】
透過プロキシを有効にします。
動作させる場合、先にNAT設定画面からNATのリダイレクト設定が必要になります。
（NATリダイレクト設定は79P）

2-4. 共通設定

共通設定			
管理者への通知設定	メールアドレス	※複数指定をする際は、指定ごとに改行入力してください。 ※最大で1999バイトまで設定できます。	
	SMTPサーバ	ホスト名	
		ポート番号	25
		検出通知メッセージの編集	
一時保存ディレクトリ		/var/tmp/virusgw	
隔離保存ディレクトリ		/var/tmp/quarantine	

■管理者への通知設定
・メールアドレス：管理者のメールアドレスを指定します。
・SMTPサーバ：管理者に検出通知をメールで送信するときに利用するメールサーバを指定します。
・検出通知メッセージの編集：ウイルス検出時に表示するメッセージを編集することができます。
（日本語での指定が可能です。）

■一時保存ディレクトリ
動作保証対象外となりますので設定しないでください。

■隔離保存ディレクトリ
動作保証対象外となりますので設定しないでください。

■スパム検査方法

カスタム条件：スパムの判定条件を個別に指定します。

スパム検査方法　カスタム条件　有効　無効

スパム条件の編集

スパム条件の編集

スパム判定条件の個別設定ができます。条件は100件まで登録できます。
設定後はプロキシ設定画面でサービスを開始してください。
条件は上から順に評価します。
検査文字列はコンマ(",")区切りで複数指定できます。

条件の追加

フィールド名:　Subject　その他
※最大で29バイトまで設定できます。

検査文字列:
※複数指定をする際は、指定ごとに改行入力してください。
※最大で800バイトまで設定できます。

比較方法:　前方一致　不一致　前の条件とAND　後方一致　大文字小文字を区別　前の条件とAND(同一MIMEパート)

判定:　スパム

条件追加場所:　一番上に追加　一番下に追加　条件　の上に追加

条件を追加

スパム条件一覧

保存　戻る

スパム条件の編集
スパムの判定条件一覧を編集します。指定条件に一致する場合スパム又は非スパムとして判定します。
カスタム条件は他の検査方法より優先され、条件のリストは上から順に判断します。

■フィールド名/その他：メールヘッダにて、フィルターのトリガーにするフィールドを設定します。

■検査文字列：上記にて設定したフィールドに入力されているトリガーとなる文字列を設定します。
■比較方法：上記にて設定した、文字列をメールヘッダの該当欄と比較する際に、どのように一致を確かめるかの方法を指定します。

■判定：上記までの条件に一致した対象をスパムとしてみるかどうかの設定を行ないます。
■条件追加場所：「条件を追加」ボタンを押して追加場所を選び、スパム条件一覧を保存します。

※設定後は、プロキシ設定画面にて「保存・再起動」をクリックしてサービスを再起動してください。

■データベース
利用するスパム検査データベースを指定できます。各データベースに基づき、スパムメールとして扱うか否かを決定します。ここで、スパムメールと認知されたものに関しては、各メールプロキシの動作設定に基づき処理されます。

メールのヘッダ情報を元に“未承諾広告”、“広告一般”、“HTML主体メール”、“ウィルス・スパム通知メール”、“エラーメール”から選択された項目をスパムメールとして判定します。
“HTML主体メール”は指定すると、画像ファイルやリンクを含むHTMLのみのメール等を検出します。

■RBL
RBL(Realtime Black List)によるスパム検査の有無と、スパム検査で参照するRBLサーバを指定します。各メールについて、接続元IPアドレス(SMTPの場合)及びReceivedヘッダに記載されているIPアドレスがRBLサーバに登録されているかすることで検査を行います。

■SURBL
SURBL(SPAM URL Realtime Black List)によるスパム検査の有無と、スパム検査で参照するSURBLサーバを指定します。各メールについて、テキスト本文とHTML本文に含まれるURLのドメイン名部分がSURBLサーバに登録されているか確認することで検査を行います。

2-5. NATリダイレクト設定

透過プロキシを使用する場合、まず使用するプロトコルにチェックを付けます。
その後、プロキシ設定画面にて、各プロトコルの「透過プロキシモード」を有効にし、
「保存・再起動」をクリックします。

3. 手動更新

「今すぐ更新」ボタンを押す事によりウイルスパターンファイルを最新に更新します。
設置時には必ず更新を行って下さい。

■プロキシサーバ
インターネットにアクセスする際、プロキシサーバを経由している場合に設定します。
プロキシサーバを経由していない場合には、無効のままで問題ありません。

手動更新

ウイルス定義ファイルバージョン		2009-08-24_10
プロキシサーバ		有効 無効
	プロキシサーバ名	ホスト名 proxy-host.xx.jp
		ポート番号 12345
	プロキシ認証	有効 無効
		ユーザ名
		パスワード

今すぐ更新

4. 自動更新

定期的(1 時間間隔)に、ウイルスパターンファイルを最新に更新します。

■プロキシサーバ
インターネットにアクセスする際、プロキシサーバを経由している場合に設定します。
プロキシサーバを経由していない場合には、無効のままで問題ありません。

自動更新

自動更新		有効 無効	
プロキシサーバ		有効 無効	
	プロキシサーバ名	ホスト名	proxy-host.xx.jp
		ポート番号	12345
	プロキシ認証	有効 無効	
		ユーザ名	
		パスワード	

保存　キャンセル

5. ログ

■アクセスログ
プロキシを経由して接続を行った記録を表示します。

■ウイルスログ
ウイルスを検出した際の記録を表示します。

■エラーログ
エラー発生時の記録を表示します。

■情報ログ
その他の一般的な情報が表示されます。

■管理画面
アンチウイルスの設定をブラウザで行ったログが表示されます。

■ウイルス定義ファイル
パターンファイルの更新履歴を表示します。

6. ウェブ管理画面のパスワード変更

ウェブ管理画面のパスワードを変更します。

管理パスワード

管理ユーザ名	admin
新しいパスワード	
確認パスワード	

保存　キャンセル

7. ライセンス情報

配布されたライセンスキーを入力します。

8. バージョン情報

本製品のバージョン情報及び利用環境を表示します。

バージョン情報

F-Secure アンチウイルス Linux ゲートウェイ	3.01
License	License OK: Valid License(for corporation)
Virus pattern file	2009-08-25_02
Engine	Hydra: 2.8.8110 AVP: 4.0.166 FMLIB: 2.0.14341 fsavd: AUA: 8.24.3035
Date	2009/08/25(Tue) 19:54:03 -0400(EDT)

環境情報

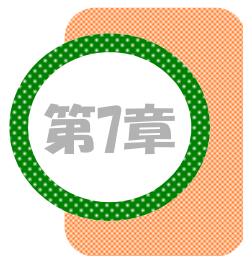
Distribution		redhat-release:Red Hat Linux release 7.3 (Valhalla)
OS		Linux xt.localdomain 2.4.20-28.7 #1 Thu Dec 18 11:15:04 EST 2003 i686 unknown
glibc		glibc 2.3.4 stable
Hardware	model name cpu MHz MemTotal MemFree SwapTotal SwapFree	VIA Nehemiah 801.845 902964 kB 315720 kB 2064344 kB 2064344 kB
Interface	eth0 eth1 lo	Link encap:Ethernet HWaddr 00:40:63:F9:7E:2A inet addr:192.168.1.1 Bcast:192.168.1.255 Mask:255.255.255.0 Link encap:Ethernet HWaddr 00:40:63:F9:7E:2B inet addr:192.168.2.142 Bcast:192.168.2.255 Mask:255.255.255.0 Link encap:Local Loopback inet addr:127.0.0.1 Mask:255.0.0.0

9. 診断情報

本製品(アンチウイルスLinuxゲートウェイ)の設定情報等を集め、圧縮ファイルを作成します。

診断情報

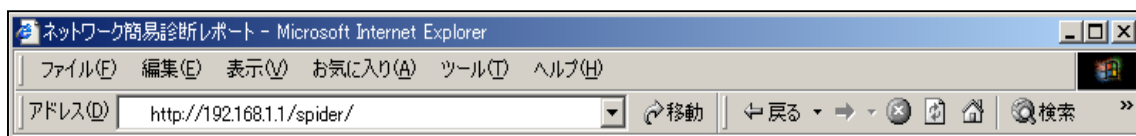
サポートへの問い合わせの際には診断情報(diag.tar.gz)をお送りください。

診断情報をダウンロード

ネットワーク簡易診断レポートへのアクセス方法

1. Webインタフェースへのアクセス

1-1. ネットワーク簡易診断レポートへのアクセス

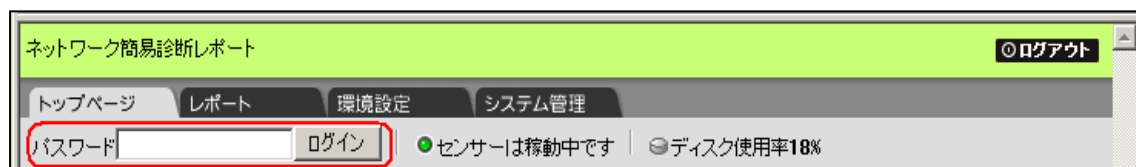
ブラウザのアドレスバーに
http://192.168.1.1/spider/と入力します。

アドレス“http://192.168.1.1/spider/”

1-2.ネットワーク簡易診断レポートへのログイン方法

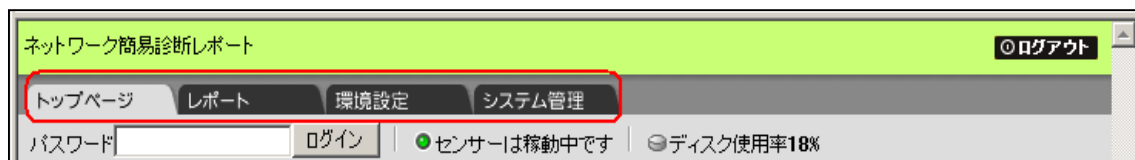
『トップページ』が表示されたら、ページ上部にある入力フォームにパスワードを入力し、
［ログイン］ボタンをクリックしてログインします。

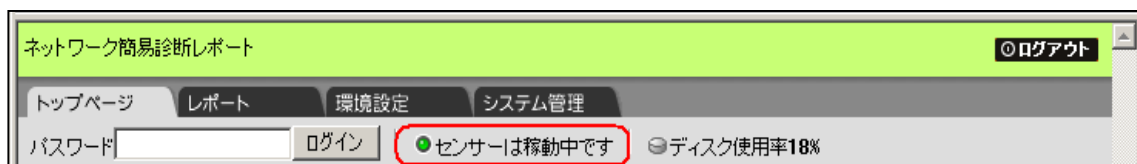
※必ず［ログイン］ボタンをクリックしてログインしてください。
［Enter］キーではログインできません。

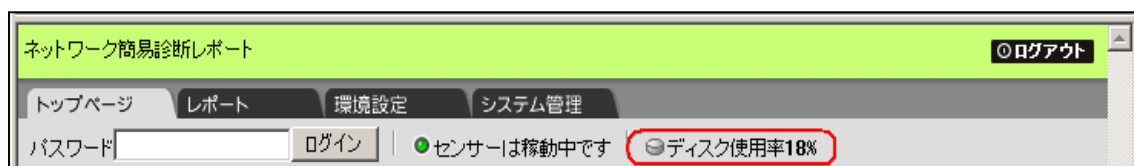
■ パスワード
［出荷時デフォルト設定：@spider@］

ネットワーク簡易診断レポート　ログアウト
トップページ　レポート　環境設定　システム管理
パスワード　ログイン　センサーは稼動中です　ディスク使用率18%

2. トップページタブ画面説明

■タブメニューボタン

［トップページ］［レポート］［環境設定］［システム管理］のタブメニューボタンで各タスクを選択します。

■センサーの稼動状況

正常にセンサーが動作している場合には「センサーは稼動中です」と表示されます。
「センサーは停止しています」と表示されている場合は、なんらかの原因でセンサーが停止しています。
センサーが停止している場合には、『システム管理』の「センサーの起動・停止」にある［センサー起動］ボタンでセンサーを起動してください。

■ディスク使用率

本製品はハードディスクにログを蓄積します。
100%で全ての領域を使っている状態になります。小数点以下は表示されないため、使用開始直後は0%のままですが異常ではありません。

3. レポートタブ画面説明

専門的な知識がなくとも解かりやすい直感的なグラフや表によるレポートを表示します。
『トラフィックの推移・傾向』『閲覧サイトの傾向』等を［日単位］、［時間単位］、
［クライアント単位］、［グループ単位］で観る事ができます。

■集計期間

①集計範囲
集計する期間を任意に入力します。
日付をハイフン“-”で区切って入力してください。一桁の場合には「0」で埋めてください。

②プリセット
月単位、週単位、日単位のプリセットから、集計する期間を選択できます。

月単位で［今月／１ヶ月前／２ヶ月前／３ヶ月前（実際の年月表示）］週単位で［今週／先週／先々週（日～土）］日単位で［今日／１日前／２日前／３日前］が選択できます。
ここで選択した期間が「集計範囲」に自動設定されます。

■曜日／時間　指定

「曜日指定」「時間指定」各プリセットを指定し、［再表示］をクリックする事で、特定の条件のみを絞込表示する事ができます。

①曜日指定

「日／月／火／水／木／金／土／平日（月～金）／土日」から指定します。

②時間指定

「午前（AM）／午後（PM）／12時台／17 ～ 23時台／18 ～ 23時台／19 ～ 23時台」から指定します。

■クライアント／特定PC

特定のPCを指定して集計する場合、項目にIPアドレスを入力します。

■再表示／リセット

再表示	リセット

①再表示
絞込条件を変更した場合に［再表示］ボタンをクリックする事で、変更設定内容が反映された結果を表示します。

②リセット
各絞込条件を［リセット］ボタンをクリックする事で、初期値にリセットする事ができます。
初期値は、「日付」が当日、「時刻」が現在時（午後3時15分の場合－15:00:00）となります。
［リセット］ボタンでは、絞込条件のみ初期値に戻すため、初期値の絞込条件の表示にするには、［再表示］ボタンをクリックします。

■レポートメニュー

「ネットワーク総合統計」「閲覧サイト順位」各項目をクリックする事で、それぞれの閲覧したいレポートを表示します。

■ネットワーク総合統計

データ量・パケット数・転送時間を総量として「Web」「メール」「ファイル転送とプリント通信」「その他」の4サービス毎に、また集計期間の総量／割合を「表」と「グラフ」で見ることができます。

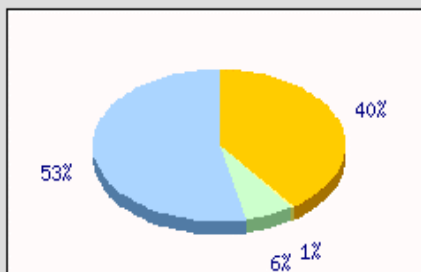
①集計条件
「集計期間」「各種指定」「クライアント」など設定した絞込条件を表示します。

期間	曜日	時間	クライアント	集計対象
2006-06-01 ～ 2006-06-30				データ量

②全体統計
「表」と「円グラフ」で「Web」「メール」「ファイル転送とプリント通信」「その他」の4サービス毎の割合を見ることができます。

全体統計

サービス分類	上り	下り	上り＋下り	割合
WEB	536 M	5.6 G	6.2 G	53.4 %
MAIL	105.5 M	616.5 M	722 M	6.2 %
FILE&PRINT	54.5 M	222 B	54.5 M	0.5 %
その他	1.5 G	3.1 G	4.6 G	39.9 %
合計	2.2 G	9.4 G	11.6 G	100 %

※上り…クライアント→サーバ、下り…サーバ→クライアント

③～⑥はそれぞれ「日別」「週別」「時間別」「クライアントPC別」毎の統計です。
表示されている各項目の中で、総量が最も多い場合に数字が「赤」で表示され、各項目毎に最も割合の高いサービスが「マーカー表示」されます。

③日別統計

■日別統計

日付	上り＋下り	W	M	F	他	相対度グラフ(最大値を100とした場合)
2006-06-02 (金)	827.2 M	57	7.6	0.2	35.1	
2006-06-03 (土)	695.2 M	77.6	8.2	0.6	13.6	
2006-06-04 (日)	280.4 M	83.4	11.8	1.5	3.4	
2006-06-05 (月)	1.8 G	45.8	6.5	0.4	47.3	
2006-06-06 (火)	1.7 G	47.5	6.6	0.5	45.4	
2006-06-07 (水)	1.3 G	52.8	9.4	0.6	37.2	
2006-06-08 (木)	2 G	39.1	3.1	0.3	57.5	
2006-06-09 (金)	1.7 G	58	5.4	0.4	36.2	
2006-06-10 (土)	487.2 M	80.4	6.2	0.6	12.8	
2006-06-11 (日)	5 M	29.5	19.6	42.7	8.2	
2006-06-12 (月)	676.6 M	59.4	3.6	0.5	36.5	

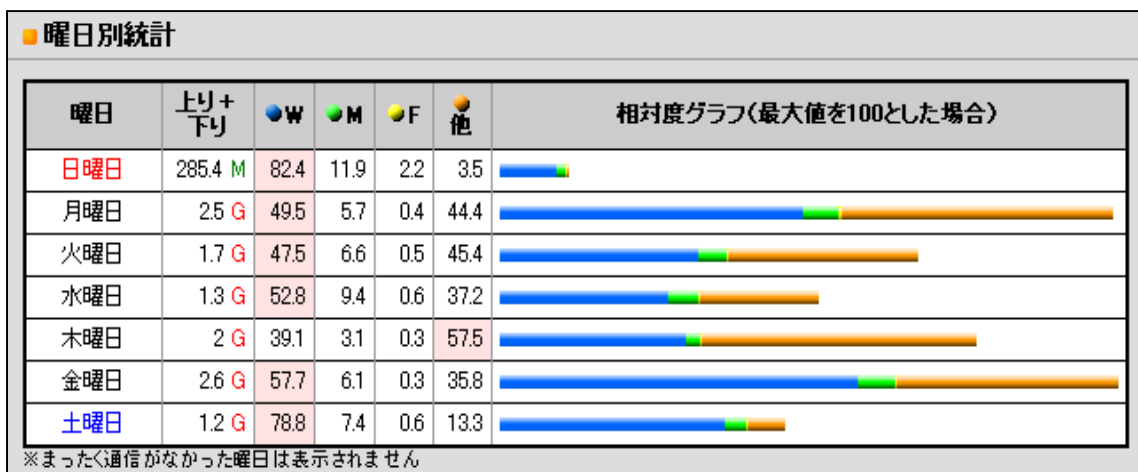
※まったく通信がなかった日付は表示されません

1日毎に統計を表示します。
通信がまったくない日は、【日付】に項目として表示されません。

④曜日別統計

■曜日別統計

曜日	上り+下り	●W	●M	●F	他	相対度グラフ(最大値を100とした場合)
日曜日	285.4 M	82.4	11.9	2.2	3.5	
月曜日	2.5 G	49.5	5.7	0.4	44.4	
火曜日	1.7 G	47.5	6.6	0.5	45.4	
水曜日	1.3 G	52.8	9.4	0.6	37.2	
木曜日	2 G	39.1	3.1	0.3	57.5	
金曜日	2.6 G	57.7	6.1	0.3	35.8	
土曜日	1.2 G	78.8	7.4	0.6	13.3	

※まったく通信がなかった曜日は表示されません

曜日毎に統計を表示します。
通信がまったくない曜日は、【曜日】に項目として表示されません。

⑤時間別統計
時間毎に統計を表示します。通信がまったくない時間は、【時間】に項目として表示されません。

■時間別統計

時間	上り+下り	●W	●M	●F	他	相対度グラフ(最大値を100とした場合)
0 時台	89.9 M	6.4	6.2	1.6	85.9	
1 時台	75.4 M	5.5	6.8	1.9	85.8	
2 時台	68.5 M	1.6	6.5	2	89.8	
3 時台	66.9 M	5.1	7.2	2.1	85.6	
4 時台	60.4 M	5.8	7.6	2.3	84.3	
5 時台	59 M	8.4	7.4	2.4	81.9	
6 時台	66.6 M	8.2	10.3	2.2	79.3	
7 時台	232.4 M	53.2	11.8	0.8	34.2	
8 時台	737.4 M	72.4	8.8	0.5	18.3	
9 時台	732.6 M	58.6	8.7	0.4	32.3	
10 時台	527.4 M	49.2	5.4	0.6	44.8	
11 時台	605.5 M	49	4.7	0.5	45.8	
12 時台	932 M	76	2.7	0.3	21	
13 時台	596.3 M	55.8	7.6	0.5	36.1	
14 時台	802 M	63.6	4.8	0.3	31.3	
15 時台	685.3 M	53.3	7.9	0.4	38.4	
16 時台	794.2 M	49	4.8	0.3	45.9	
17 時台	1 G	54.1	6.3	0.4	39.2	
18 時台	1.1 G	47.9	7.1	0.3	44.7	
19 時台	643 M	59.4	7.3	0.4	32.8	
20 時台	742.6 M	50.2	3.5	0.3	46	
21 時台	610.2 M	41.9	4.1	0.3	53.7	
22 時台	251.2 M	41.6	9.5	0.7	48.2	
23 時台	79.1 M	13.1	11	1.9	74	

※まったく通信がなかった時間は表示されません

■閲覧サイト順位

閲覧（アクセス）したサイトを接続回数による順位で表示します。

①集計条件

「集計期間」「各種指定」など設定した絞込条件を表示します。

期間	曜日	時間	PC	ベースURL
2006-06-01 ～ 2006-06-30				

②閲覧サイト順位

閲覧（アクセス）したサイトを接続回数による順位で表示します。

順位	ベースURL	接続回数
1	http://i.yimg.jp/	24538
2	http://ai.yimg.jp/	20544
3	http://img.yahoo.co.jp/	15836
4	http://bc.yahoo.co.jp/	13276
5	http://ca.c.yimg.jp/	10477
6	http://www.lis-fss.co.jp/	7717
7	http://www.mapfan.com/	7146
8	http://rikunabi-next.yahoo.co.jp/	6997
9	http://image.rakuten.co.jp/	5382
10	http://mail.google.com/	4111
11	http://image.www.rakuten.co.jp/	4097
12	http://avupdate.F-Secure.com/	3883
13	http://image.itmedia.co.jp/	3666
14	http://download.windowsupdate.com/	3644
15	http://update.microsoft.com/	3628
16	http://www.nttdocomo.co.jp/	3589

4. 環境設定画面説明

■環境設定

『環境設定』では、PC情報登録、プロトコルの設定、URLの管理、ネットワークに関する設定、ソフトウェアに関する設定を行います。

■ソフトウェア関連設定

●プロキシサーバ

インターネットにアクセスする際、LAN内及びLAN外のプロキシサーバを経由している場合に設定します。

プロキシサーバを経由していない場合には、空欄のままで問題ありません。

設定する場合には、プロキシサーバの「IPアドレス」と「ポート番号」をコロン(:)でつないで入力し、［入力値チェック］ボタンをクリックします。

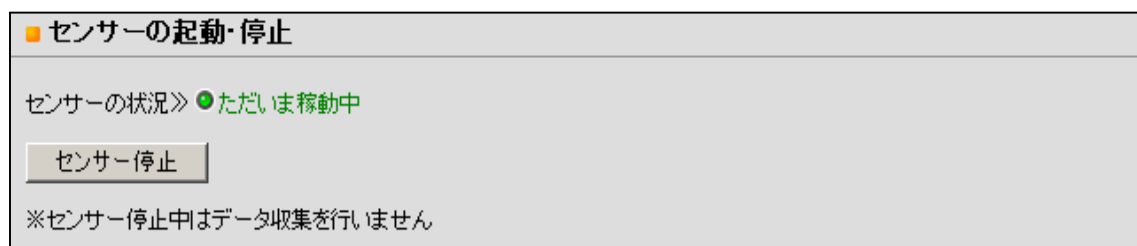
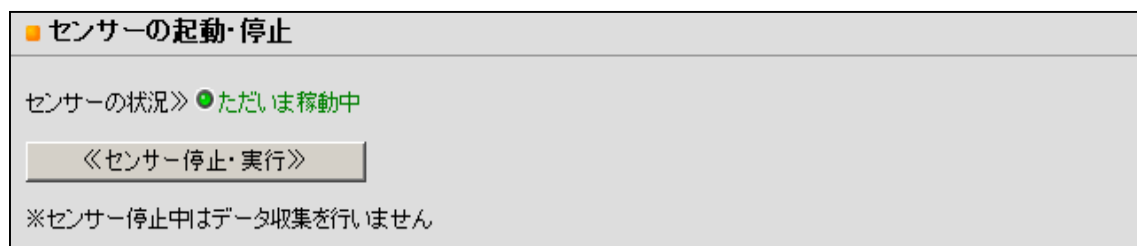
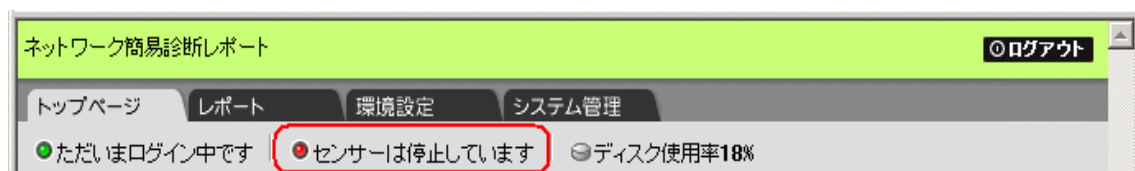
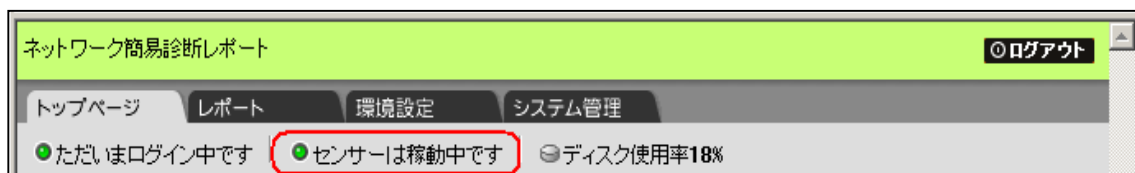
同じ位置に［センサー再起動・実行］ボタンが表示されますので、クリックしてセンサーを再起動してください。

センサー再起動後設定が反映されます。

5. システム管理画面説明

『システム管理』では、本製品のシステムに関する設定をします。

■センサーの起動・停止

センサーを一時的に停止する事ができます。

センサー起動時には［センサー停止］ボタンが表示され、センサー停止時には［センサー起動］ボタンが表示されます。

各ボタンをクリックすると、同じ位置に［センサー起動／停止・実行］ボタンが表示されます。この［センサー起動／停止・実行］ボタンをクリックすると「停止」もしくは「起動」状態となります。

センサーの動作状況は『トップページ』の上部にも表示されます。 センサー起動時は「センサーは稼動中です」、センサー停止時は「センサーは停止しています」と表示されます。
センサー停止中は、ログビューアのデータが収集されません。

■ログインパスワード変更

セキュリティや運用上、パスワードの変更が必要な場合に設定します。

入力フォームに新しいパスワードを入力し、［入力値チェック］ボタンをクリックします。
同じ場所に表示される［パスワード変更・実行］ボタンをクリックしてください。
変更したパスワードは、［ログアウト］後有効になります。

※パスワード変更した場合、変更したパスワードの確認手段がありませんので、パスワード変更する際には、変更パスワードを忘れる事のないよう十分ご注意ください。

※変更パスワードを忘れた場合には、本製品のWebインタフェースを使用する事ができません。そのためコンソールから出荷時設定に戻す必要があります。

※パスワードは半角英数5 ～ 8文字以内で設定してください。

■データの取出し

各データの取出し（バックアップ）時に利用します。
各項目のバックアップファイルを任意のハードディスクへ取出す（保存）ことが出来ます。

データの取出し

N/W総合統計	SP2_NrepoA.pgs	取出し
閲覧サイト順位	SP2_WrepoB.pgs	取出し

※注意点
・取出しを行っても、ディスク内のデータは削除されません

それぞれの項目は次の通りです。

● NRレポートA［SP2_NrepoA.pgs］
［NR］『レポート』の「ネットワーク総合統計データ」バックアップファイル

● WebレポートA［SP2_WrepoA.pgs］
［Web］『レポート』の「Web利用統計データ」バックアップファイル

■データの取出し（バックアップ）

［取出し］ボタンをクリックすると、該当ファイルのダウンロードダイアログが表示され、
各テーブルのバックアップファイルを任意のハードディスクへ保存する事ができます。

■ログデータの削除

「ログビューア」「レポート」のデータを削除します。

ログデータの削除

ログデータ削除・確認

※削除対象:レポート内の全データ

削除したデータは、復元する事ができませんのでご注意ください。
長期間蓄えたログデータは、削除するのに時間がかかる場合があります。
「PC登録」「ベースURL管理」「プロトコル登録」の各データは削除されません。

■ お問い合わせの前に

本書をよくお読みになり、問題が解決できないか御確認ください。

ネットワーク構成情報は本製品設置時に弊社へお知らせください。

お問い合わせの際にネットワーク構成情報と問題の症状を合わせてお知らせいただくことで、問題の解決が早まることがあります。

■ お問い合わせ窓口

アルテミス　サポートセンター
TEL：03-3435-7567
FAX：03-3435-9416

■ 製品仕様

（）内は***Appliance α***の仕様になります。

OS	Red Hat Linux 7.3
CPU	VIA C3 800MHz(VIA C3 1.0GHz)
メモリ	1GB(1GB)
HDD	40GB×1(80GB×1)
NIC	10/100Mbps Ethernet×2
外形寸法(mm)	215×253×55(215×300×70) / 幅×奥行×高さ
重量	2.5kg(4kg)

X-Terminator αシリーズ
取扱説明書
Ver. 2.0
発行日　2009年8月27日
発行責任　株式会社アルテミス